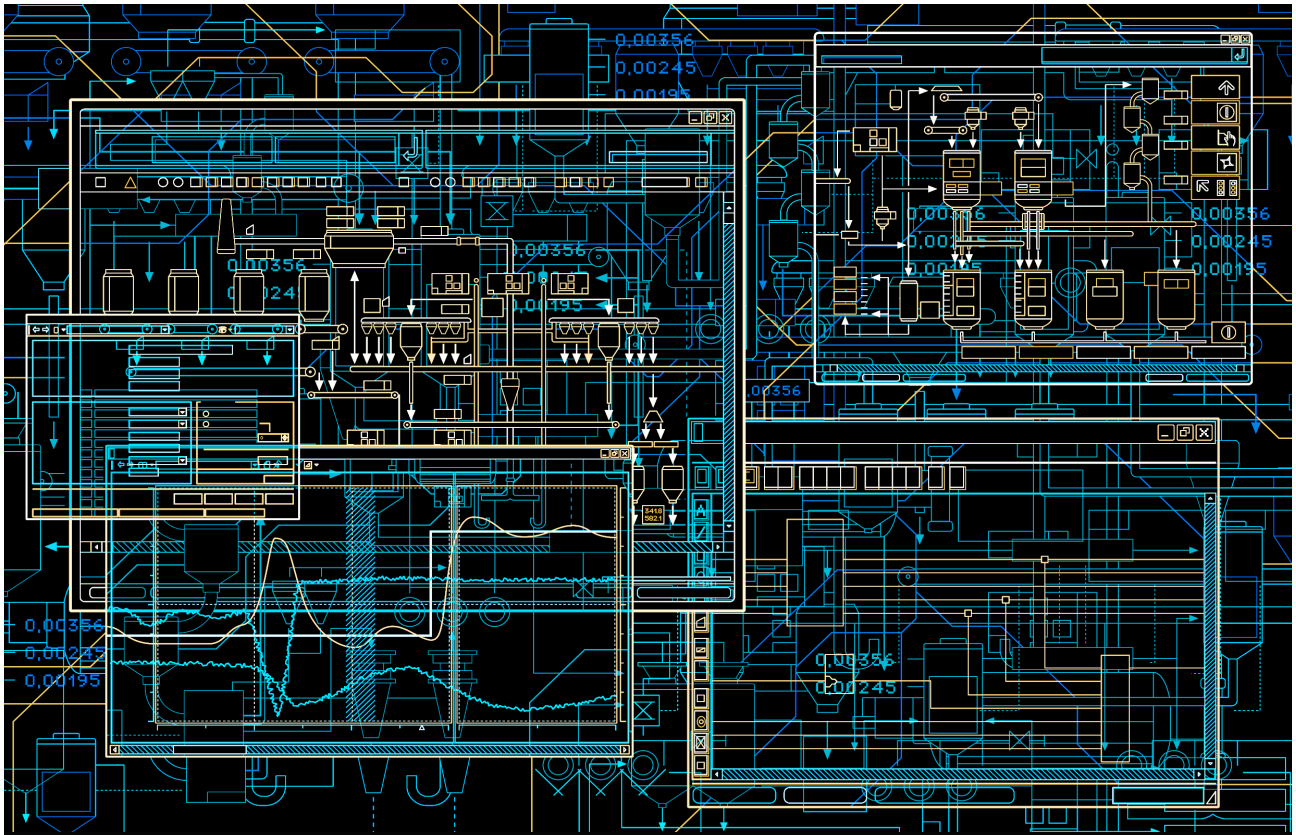

System 800xA

Virtualization with VMware vSphere ESX

System Version 5.1

Power and productivity
for a better world™

System 800xA

Virtualization with VMware vSphere ESX

System Version 5.1

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2003-2013 by ABB.
All rights reserved.

Release: February 2013
Document number: 3BSE056141-510 F

Table of Contents

About This User Manual

User Manual Conventions 12
Warning, Caution, Information, and Tip Icons 12
Terminology 12
Released User Manuals and Release Notes 13

Section 1 - Introduction

Overview of Virtualization 15

Section 2 - 800xA Server Node Consolidation

Non-virtualized 800xA System 17
Consolidated 800xA System 18

Section 3 - Planning

System Planning 21
Determine Required VMware ESX(i) Server Hardware 22
Determine Additional Hardware 25
    800xA Licensing Dongle 25
    Connecting the 800xA USB Licensing Dongle to the CLS Server 25
    Using the ABB USB Dongle Over the Network 26
    800xA for Advant Master and 800xA for MOD 300 27
VMware vSphere ESX Versions 28
    VMware ESXi Server 28
    VMware ESX Server 29

Section 4 - Installation and Configuration

VMware ESXi 5.0 Server Installation 31
VMware ESX Server Installation 37
VMware ESXi 4.1 Server Installation 40
vSphere Client Installation 42
Setting ESX(i) time 43
Set Up 800xA Server Nodes as VMs 44
Create Virtual Switches 44
Create VMs and Connect them to Virtual Switches 46
Install 800xA into the VMs 47

Section 5 - Backup and Restore

Backup and Restore of an ESX(i) Server 51
Backup and Restore of Virtual Machines 52

Section 6 - Security

Roles 53
Users 54
Permissions 55

Section 7 - Optimizations

Virtual CPUs 57
Allocating Virtual CPUs to Physical Cores 58

Section 8 - Monitoring VMware vSphere ESX(i)

Setup the Network Connections 59
Supported Hardware for Virtualization 59
Dell and HP Servers 60
IBM Servers 62
Adding Vendor Management Software 63
Monitoring Dell R710 Running VMware vSphere ESX 64
Pre-requisites 64
Procedure Summary 64
Configure Networking of ESX and 800xA AO Server 64

Installing Dell OpenManager Server Administrator Managed Node....65
Adding Support for Dell R710 to System 800xA....66
Configuration....67
Confirmation: Test the Configuration....68
Monitoring HP DL380 G6 Running VMware vSphere ESX....69
Pre-requisites....69
Procedure Summary....69
Configure Networking of ESX and 800xA AO Server....69
Install and Configure HP System Management in the ESX Server....69
Installation Sequence....71
Adding ABB Object Types....78
Creating Objects....78
Configure the Object....79
Monitoring IBM x3650M2 Running VMware vSphere ESX....80
Pre-requisites....80
Procedure Summary....80
Configure Networking of ESX and 800xA AO Server....80
Configure the ESX Server....80
Adding ABB Object Types....81
Creating Objects....81
Configure the Object....82
Monitoring SNMP Traps in ESXi Server....82
Configuring IT SNMP Trap Service....83

Section 9 - Installing VMware CLI, Drivers, Updates and Upgrades

VMware Command Line Interface....91
Installing VMware Command Line Interface....91
Installing Drivers....93
Identify Hardware Requiring Additional Drivers....93
Download Driver from VMware....93
Prepare the ESX Server....93
Restart System and Start Guests....95

Section 10 - Upgrading ESX 4.0 Update 1 to ESX 4.1

Download Upgrade Files 97
Prepare ESX Server 98
Apply Upgrades 98
Restart System and Start Guests 99
Install the vSphere Client 4.1 99
Upgrade VMware Tools in the Guests 100
Changes from ESX 4.0 Update1 to ESX 4.1 100
    USB Memory Sticks 100

Section 11 - Supported 800xA Server Node Types

Support Components 101
Application Servers 102
Connectivity Servers 102
Parts List 103
    Redundant 4 Node 800xA System 103
    Redundant 8 Node 800xA System 105
    Additional External Parts 107

Section 12 - Storage Area Network

SAN Hardware 110
SAN Storage Configuration 111
SAN Networking 112
ESX Server Network Configuration 117
    Adding in Datastores 117

Section 13 - VMware vCenter Server

User Accounts 125
Installation Procedure 126
    Pre-requisites 126
    Installing vCenter Server 126
    Installing vSphere Client 127
    Configuring vCenter Server 128

Adding a Datacenter Object 128
Adding an ESX(i) Server 128
Limitations when Interacting with ESX(i) Servers 129

Section 14 - Improving Availability

Configuring VMware High Availability 131
Adding a Cluster Object 132
Adding ESX(i) Servers to the Cluster 133
Specifying Failover Host 133
VMware vMotion 135
VMware Storage vMotion 135
VMware Fault Tolerance 135

Section 15 - 800xA in the IT Infrastructure

Section 16 - Virtual Client

Virtual Terminal Server 141
Benefits of Virtual 800xA Workplaces 142
Comparison of Virtual Client and Virtual Terminal Server 143
Control Room Planning 143
Graphical Presentation and Physical Server Speed 144
Configuring the Virtual Client Virtual Server Hardware 144
Virtual Client 145
VMWare ESXi Server Dimensioning for Virtual Clients 146
Configuring the Virtual Terminal Server Virtual Server 146
Terminal Server Definition 147
VMWare ESXi Server Dimensioning for Virtual Terminal Servers 148
Thin Clients 149
Multiple Screen 150
Limitations 151

Appendix A - ESX(i) Host Setup Check List

Appendix B - ESX(i) Guest Setup Check List

Appendix C - Further Technical Information on VMware ESX(i)

Index

Revision History

Updates in Revision Index A 162
Updates in Revision Index B 162
Updates in Revision Index C 163
Updates in Revision Index D 164
Updates in Revision Index E 164
Updates in Revision Index F 165

About This User Manual

Any security measures described in this User Manual, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

This User Manual provides an overview of virtualization and how it is to be used with 800xA through the following topics:

- Overview of virtualization.
- 800xA server node consolidation based on VMware ESX(i).
- Consolidating 800xA server nodes on VMware ESX(i) servers.
- System planning, installation, and configuration using VMware ESX(i).
- Backup and Restore of a virtualized system.
- Security.
- Optimizations.
- Monitoring VMware vSphere ESX(i).
- Upgrading from ESX 4.0U1 to ESX 4.1.
- Supported 800xA node types.
- SAN Storage Server.
- vCenter Server.
- VMware High Availability.

User Manual Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Warning, Caution, Information, and Tip Icons

This User Manual includes Warning, Caution, and Information where appropriate to point out safety related or other important information. It also includes Tip to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard that could result in *electrical shock.*

Warning icon indicates the presence of a hazard that could result in *personal injury.*

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard that could result in *corruption of software or damage to equipment/property.*

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although Warning hazards are related to personal injury, and Caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, fully comply with all Warning and Caution notices.

Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018*).* The listing includes terms and

definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as Webster's Dictionary of Computer Terms.

Released User Manuals and Release Notes

A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in *System 800xA Released User Manuals and Release Notes (3BUA000263*)*.

System 800xA Released User Manuals and Release Notes (3BUA000263)* is updated each time a document is updated or a new document is released. It is in pdf format and is provided in the following ways:

- Included on the documentation media provided with the system and published to ABB SolutionsBank when released as part of a major or minor release, Service Pack, Feature Pack, or System Revision.
- Published to ABB SolutionsBank when a User Manual or Release Note is updated in between any of the release cycles listed in the first bullet.

A product bulletin is published each time *System 800xA Released User Manuals and Release Notes (3BUA000263*)* is updated and published to ABB SolutionsBank.

Section 1 Introduction

As the use of virtualization has expanded dramatically in the business and financial sector amongst others, ABB is now providing the ability to take advantage of virtualization in the process industries. Virtualization can be used in 800xA systems to combine multiple 800xA server nodes onto a single computer. The total number of physical computers required in an installation is reduced significantly. This also reduces the required space for computers, hardware acquisition cost for computers and cabinets, and operating costs (such as energy costs).

Overview of Virtualization

VMware ESX is a virtualization technology that enables running multiple virtual machines (VM) on the same physical computer. Each VM represents a computer and its hardware components (CPU, RAM, disk drives, network adapters, etc.). Each VM requires an operating system and applications to be installed in the same manner as a physical computer. The VM appears to the operating system as a physical computer.

Each VM requires a licensed copy of the Windows® operating system.

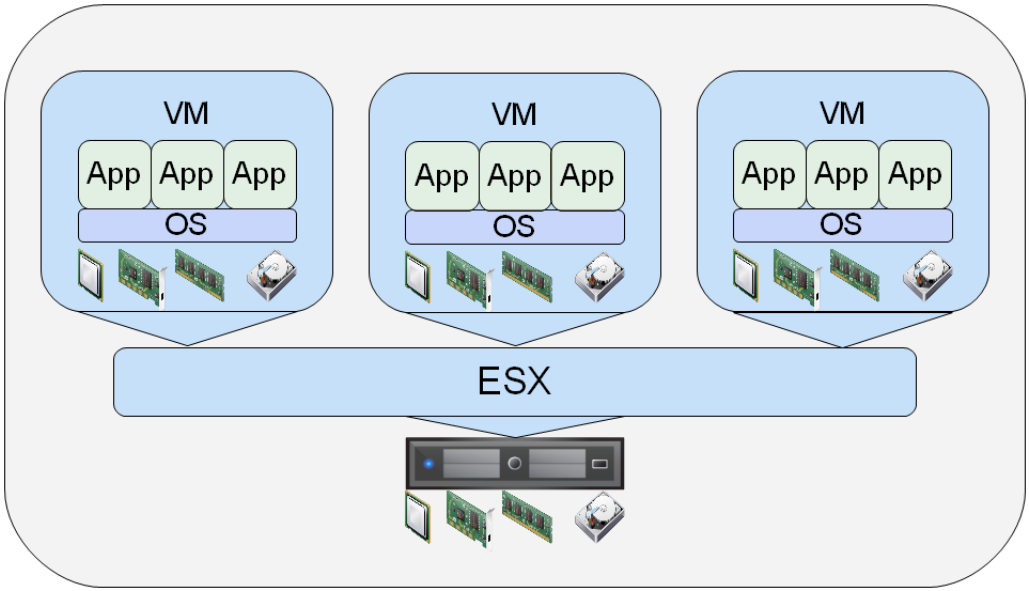

Figure 1. VMware ESX Virtualization Overview

While ESX can provide the environment that represents a computer, there are limitations regarding the types of resources made available. When planning a virtual environment, only server nodes that communicate over the network should be included.

Interaction with the virtual machines is normally performed through a dedicated client to create, modify, start and stop the virtual machines. It also enables the opening of a console to takeover the virtual machine.

VMware vSphere encompasses the VMware ESX(i) server with the advanced functionality of VMotion, High Availability, Fault Tolerance and Storage Motion. vCenter Server provides central administration of the ESX(i) servers. VMware vSphere Client is a Windows application which is used to login to the ESX(i) server, or the vCenter Server for administration purposes.

Section 2 800xA Server Node Consolidation

This section describes the details of 800xA Server Node Consolidation.

Non-virtualized 800xA System

The difference between a non-virtualized 800xA system and a VMware ESX(i) system is that some, or all, of the 800xA server nodes, run inside VMs.

For example, a non-virtualized 800xA system would be as follows (Figure 2):

- One redundant pair of Domain Controllers.
- One redundant pair of Aspect Servers.
- Three redundant pairs of Connectivity Servers for AC800M, including two Asset Optimization Servers.
- One redundant pair of FoundationFieldbus Connectivity Servers, including one Asset Optimization Server.
- Two Information Management Servers.
- Client nodes.

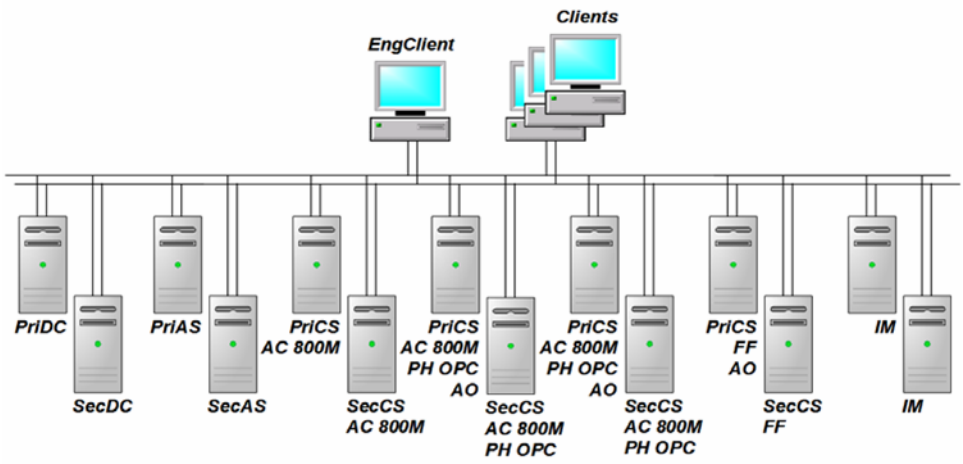

Figure 2. Example of a non-virtualized 800xA System

Consolidated 800xA System

Using VMware ESX(i), the same system can be set up (consolidated) as follows:

- One primary VMware ESX(i) server containing all primary 800xA server nodes as VMs.
- One secondary VMware ESX(i) server containing all secondary 800xA server nodes as VMs.
- Clients and engineering clients are not virtualized, but remain on physical computers.

A separate client application (VMware vSphere Client) is used for configuring the VMware ESX(i) server (for creating VMs or changing their virtual hardware). The vSphere Client is required to be installed on at least one physical computer running Microsoft Windows. This can be an 800xA Client node, preferably an Engineering Client node.

The resulting 800xA system configuration based on VMware ESX(i) is shown in Figure 3.

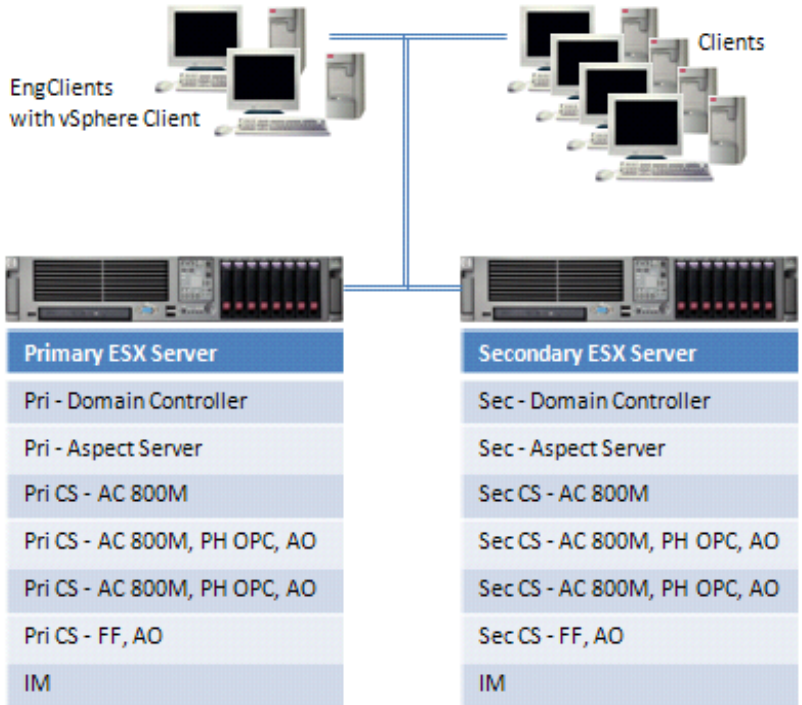
EngClients
with vSphere Client
Clients
Primary ESX Server
Pri - Domain Controller
Pri - Aspect Server
Pri CS - AC 800M
Pri CS - AC 800M, PH OPC, AO
Pri CS - AC 800M, PH OPC, AO
Pri CS - FF, AO
IM
Secondary ESX Server
Sec - Domain Controller
Sec - Aspect Server
Sec CS - AC 800M
Sec CS - AC 800M, PH OPC, AO
Sec CS - AC 800M, PH OPC, AO
Sec CS - FF, AO
IM

Figure 3. Example of a virtualized 800xA System

Compared to the non-virtualized system shown in Figure 2, which requires 14 physical servers, the virtualized system requires only two physical servers. 800xA server nodes are installed and configured into the VMs the same way physical computers are by using the 800xA System Installer tool. However, setting up

virtualized 800xA server nodes requires added steps to initially set up the VMware ESX(i) servers. This procedure is outlined in Figure 4.

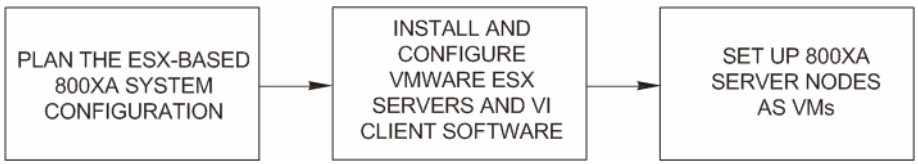
PLAN THE ESX-BASED 800XA SYSTEM CONFIGURATION
INSTALL AND CONFIGURE VMWARE ESX SERVERS AND VI CLIENT SOFTWARE
SET UP 800XA SERVER NODES AS VMs

Figure 4. Setup Procedure for VMware ESX(i) 800xA System

Each step of this procedure is discussed in detail in the following sections:

- Section 3, Planning.
- Section 4, Installation and Configuration.
- Setting ESX(i) time on page 43.

Section 3 Planning

This section describes how to plan the features, size, and configuration of the VMware ESX(i)-based 800xA system. The objective is to determine the hardware and software requirements for VMware ESX(i) servers to make the right purchases.

System Planning

The first stage to planning the system is to confirm that the required server node types are supported for virtualization. This is documented in the *System 800xA 5.1, 5.0, 4.1, 3.1 Third Party Software (3BUA000500*).*

Essentially, the configuration and dimensioning rules for 800xA server nodes stated in the *System 800xA System Guide Technical Data and Configuration (3BSE041434*)* instruction should be kept the same when the node is installed inside virtual machines. Given that these rules are followed, with additions and limitations given in this document, the performance data stated in the system guide will be fulfilled.

Use the 800xA System Planner tool to determine the types and number of 800xA nodes for a system.

For high system reliability, it is required to use two VMware ESX(i) servers - one primary and one secondary - as shown in Figure 3. Place all primary 800xA server nodes on the primary VMware ESX(i) server and place the secondary 800xA server nodes on the secondary VMware ESX(i) server. If one VMware ESX(i) server fails, all redundant 800xA server nodes on the other VMware ESX(i) server are available.

Do not place primary and secondary 800xA server nodes on the same VMware ESX(i) server (single point of failure).

The 800xA system configuration rules state that some server nodes may not be combined such as Information Management with Foundation Fieldbus. However, it

is possible to combine these nodes as separate VMs on the same physical VMware ESX(i) server because they still run as separate nodes (separate VMs). Combined server node types with heavy resource usage should be split into separate VMs to prevent resource starvation. Refer to the *System 800xA System Guide Technical Data and Configuration (3BSE041434*)* instruction for more information.

Determine Required VMware ESX(i) Server Hardware

Refer to ABB certified hardware listings for supported hardware.

Where there is a requirement for using non ABB listed server hardware, the following issues must be fully understood:

- Technical support from ABB will be limited.
- The hardware chipset must still be Intel based.
- The hardware must be in VMware's approved compatibility listings.
- There will be no support for monitoring the ESX(i) server using 800xA PNSM. This must be handled by an alternative method.

Determine the total hardware size of one VMware ESX(i) server by summing up the required performance and capacity numbers of each 800xA server node that run as VMs on the VMware ESX(i) server. Additionally, extra hardware capacity for the VMware ESX(i) server itself must be provided resulting in the following hardware size calculation rules:

- **Total RAM**: Sum up the RAM required for all virtual 800xA server nodes running on the VMware ESX(i) server. Also, add one additional gigabyte for the VMware ESX(i) server itself.

  Note that when a server has 2 CPUs, there is normally two areas for memory. One for each of the CPUs. Each of these areas should be populated with the same amount of memory. For example, if it was decided to have 20GB of memory, this would be 5 x 4GB modules. There would be 2 modules for one CPU and 3 modules for the other. The correct configuration would be to have 24GB of memory, in two sets of 3 modules.

- **Total disks**: Each VM requires a separate physical disk of type SCSI or SAS to optimize performance. The Domain Controller can be stored on the same disk where the VMware ESX(i) server software is installed.

Supported server models can be equipped with up to 16 disks. For higher reliability, it is recommended to mirror disks using RAID 1. This leaves up to eight productive disks for up to eight VMs per each VMware ESX(i) server.

- **Total CPUs**: It is recommended to have two virtual CPUs per virtual machine. It is also recommended to have one logical processor in the hardware for each virtual CPU in the virtual 800xA server nodes running on the VMware ESX(i) server. For example, two QUAD core CPUs will support 8 VMs if each VM is allocated one virtual CPU. On servers with Intel 5600 series processors of model 5620 and above, the CPU also has hyper-threading. Hyper-threading provides two logical processors per physical core and should not be considered the equivalent of a CPU core since it shares CPU resources. However, this provides more places for execution. If all physical CPU resources are in use, a virtual machine may need to wait before it is provided access to the physical CPU. Some versions of the CPU are 6 core processors instead of 4 core which also increases the number of logical processors. Hence, a dual 6 core CPU will provide 24 logical processors. In general the following should be observed:

$$\sum(Virtual\ CPUs) \leq \sum(Physical\ Logical\ Processors)$$

Where the number of VMs exceeds the number of cores available, an additional CPU, or ESX(i) server must be budgeted for. Licensing for ESX(i) 3.5/4.x server is based on a per CPU cost. With the introduction of ESXi 5.0, licensing is based on per CPU and amount of virtual RAM. Note that the ESXi 5.0 free version is restricted to 32GB physical RAM. It is essential to confirm performance requirements and to consider possible additional VMs, or increased workloads in the future before using the virtualized system in production.

In some cases, a virtual machine may have a work load that will require additional virtual CPUs to be added to the virtual machine.

- **Total Network Interface Cards (NIC)**: One separate gigabit Ethernet port is required for each physical network in which the VMware ESX(i) server should

be connected to. Additionally, one more gigabit Ethernet port is required for the VMware ESX(i) Service Console.

The number of physical network ports is limited by the hardware, and by the number of ports on the network cards used. The actual verification case described in this document used 10 hardware ports. In some cases the configuration may require more physical ports. Note that the theoretical max given by the hardware limitation may be overridden by other resource limitations. From ESX 4.0 each virtual machine can have a maximum of ten virtual ports, refer Section 16, Further Technical Information on VMware ESX(i).

Refer to the *VMware Compatibility Guide* (http://www.vmware.com/resources/compatibility/search.php) for any specific VMware ESX(i) hardware configuration constraints for the VMware ESX server model.

Determine Additional Hardware

800xA Licensing Dongle

From System 800xA 5.1 revision, VMware vSphere ESX(i) 4.1 is supported. This version of ESX(i) introduces support for physical USB devices being recognized in virtual machines. Previously, an AnywhereUSB device was required for this functionality. Note that where the virtual machine is to be moved to another server, the USB dongle must be moved and the configuration must be reviewed in the ESX(i) server and the virtual machine. In some circumstances, it still may be beneficial to have the USB dongle available over the network.

VMware ESXi does not support a physical parallel port connection. The ABB Parallel Port License Dongle cannot be used for ESXi.

In physical 800xA nodes, an ABB 800xA USB licensing dongle is attached to the computer where the 800xA CLS service is running.

Connecting the 800xA USB Licensing Dongle to the CLS Server

To enable the virtual machine to access the USB dongle the following must be done:

- Edit the settings of the virtual machine.
- Add Hardware of Device Type USB Controller. The configuration must be allowed to complete before adding USB devices.
- Insert the ABB USB Dongle into the ESX(i) Server.
- Add Hardware of Device type USB Device.
- Add relevant ABB Licence dongle USB device type from the devices listed.
- Select **Next > Finish** and then **OK**.
- Start the virtual machine. Refer to CLS Server configuration details to complete the configuration.

Using the ABB USB Dongle Over the Network

Where it may be likely to move the license server to another ESX(i) server, using the ABB dongle over the network is an advantage. With this configuration, it would not be necessary to move the dongle to the new ESX(i) server.

As shown in Figure 5 below, the AnywhereUSB is a device which has ports for USB dongles and an Ethernet port for network connectivity.

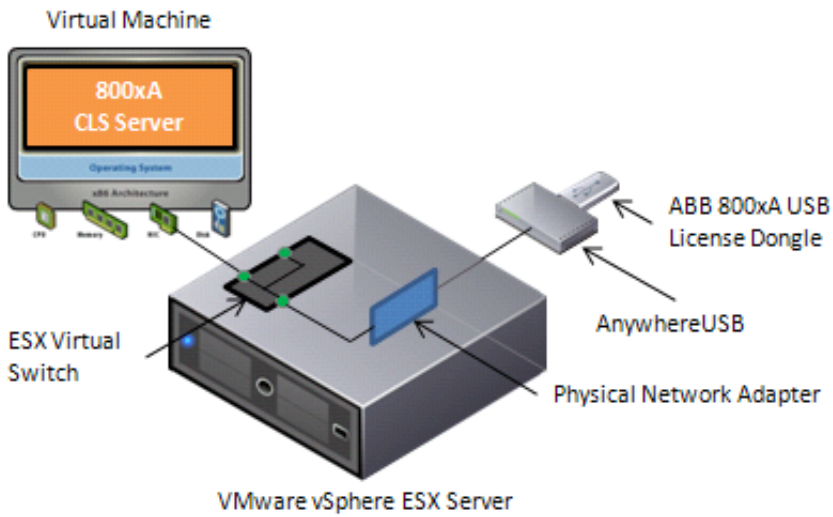

Figure 5. Connection of 800xA USB license dongle to CLS server using AnywhereUSB

Tying the 800xA license to a network card MAC address is not supported when running in a virtual environment.

800xA for Advant Master and 800xA for MOD 300

In the case of physical Connectivity Server nodes for 800xA for Advant Master and 800xA for MOD 300, an RTA board or RTA unit is used to provide connectivity to respective networks.

Hardware requiring separate drivers is usually not supported in virtual environments. This is solved by using the PU410 respectively PU412 RTA Units which is external to the ESX(i) server and communicates with it via an Ethernet link.

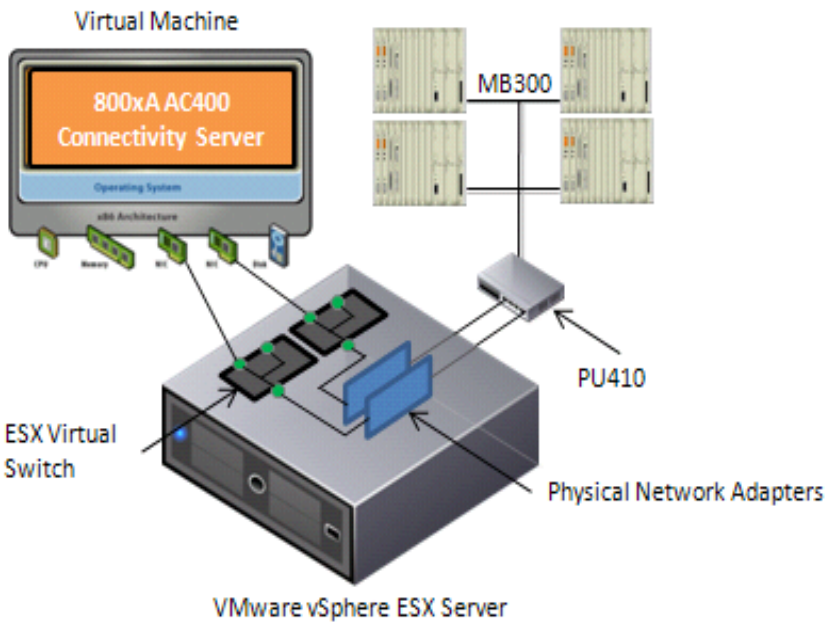

Figure 6. Example connection of 800xA for Advant Master Connectivity Server to MasterBus

VMware vSphere ESX Versions

Refer to *System 800xA 5.1, 5.0, 4.1, 3.1 Third Party Software (3BUA000500)* and *Security Updates Validation Status for System 800xA (3BSE041902)* for specific versions of ESX(i) and supported patch levels.

It is recommended to use:

ESXi 5.0 as 800xA 5.1 Revision B supports ESXi servers.

ESX 4.1 as 800xA Systems prior to 800xA 5.1 Revision B supports ESX servers.

From the introduction of the 5.0 version of VMware ESX(i) product line, VMware only provides the ESXi version. In line with the requirements to monitor the server hardware, ABB has, with the introduction of 800xA 5.1 Rev B, added the ability to receive SNMP Trap messages from ESXi servers. This provides the continued support required for the production environments.

VMware ESX 4.1, ESXi 4.1 and ESXi 5.0 are supported for System 800xA. Before selecting ESX or ESXi, the differences outlined in the following sections must be understood. VMware ESX/ESXi 4.1 and later versions requires 64-bit processor.

VMware ESXi Server

VMware ESXi server is a slimmed down version of ESX that does not contain the **service console**. In ESX, the **service console** is used to install third party applications, logon to the ESX server remotely using **ssh**, and run consolidated backups. It also supports the use of SNMP which is essential for PNSM. As of 800xA 5.1 Rev B, PNSM SNMP Trap support can be used to monitor ESXi 5.0 servers.

VMware ESXi server has the same capabilities for running virtual machines as the ESX. Installation of VMware ESXi server can be done to the local hard disk, USB, or SDHC memory device. Some vendor servers are equipped with internal SD and USB storage connectors which can be used to run ESXi. VMware ESXi server can be downloaded from VMware at no cost. Some hardware vendors (HP, Dell, IBM) also produce builds which can be downloaded from the same location in the VMware web site that include improved monitoring of hardware such as RAID storage from the vSphere Client. Basic configuration of the ESXi server is performed though the direct console displayed on the monitor connected to the

ESXi server. This is required for the initial setting of the administrative (root) password, and the IP address of the ESXi server. While VMware ESXi free version does not support the advanced functionality of ESX such as vMotion and high availability, these features can be unlocked by adding a full ESX license to the ESXi server. ESXi only supports up to 6 cores per processor 4.x versions.

VMware ESXi server does not support the VI Web Access.

VMware ESX Server

VMware ESX 4.1 Standard is the recommended supported virtualization software for running 800xA server nodes virtualized prior to 800xA 5.1 Rev B. VMware ESX server is an enterprise ready virtualization environment from VMware. It installs directly on top of the physical server and runs multiple virtual machines simultaneously sharing the physical resources of the underlying server. Each virtual machine in ESX has a BIOS, processors, ram, disk storage, and networking devices where operating systems and applications can be run unmodified. Licensing for VMware ESX is per processor (occupied socket). VMware ESX supports a Console Operating System (COS) where administrators can login for maintenance purposes. The COS is running as a virtual machine in the ESX server. It supports installing third party software. VMware ESX is managed through the vSphere Client which runs on a Windows computer. In addition to the vSphere Client, VMware ESX also has a VI Web Access that allows for interaction with the virtual machines from a web browser.

Section 4 Installation and Configuration

This section describes how to install and configure the VMware ESX(i) server and the vSphere Client software for virtual 800xA server nodes. For general information about the VMware ESX server installation, refer to the *VMware ESX Server 4.1 Get Started* manual.

http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_get_start.pdf

For the VMware ESXi Server 5.0 Installation Guide, refer to *vSphere Installation and Setup* manual.

http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-501-installation-setup-guide.pdf

VMware ESXi 5.0 Server Installation

While servers can come pre-installed in the ESXi, the following outlines the procedure for a new installation.

The following procedure is only for new installations. It is not recommended to upgrade though it is available, due to the possible interference with the configurations in the ESX(i) servers.

Many modern servers are designed with internal USB or SD slots. When extracted with a memory device, they can be used for the installation destination of ESXi.

Perform the following to install VMware ESXi server software:

1. Start the **standard installer** from the ESXi installer (Figure 7).
2. From the *Welcome to the VMware ESXi 5.0.0* Installer window, press **Enter** to Install (Figure 8).
3. Read the *End User License Agreement*, then click press **F11** to accept and continue (Figure 9).

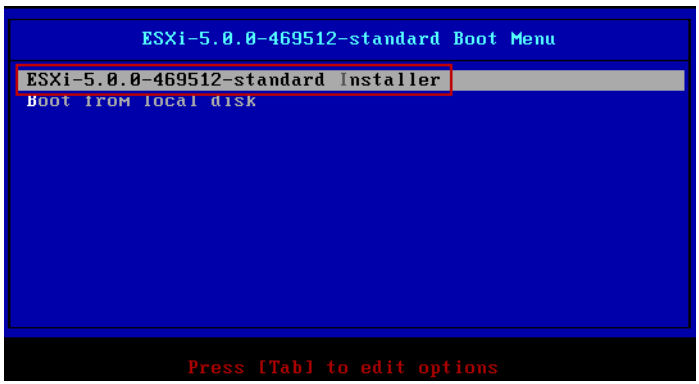

Figure 7. ESXi Installer

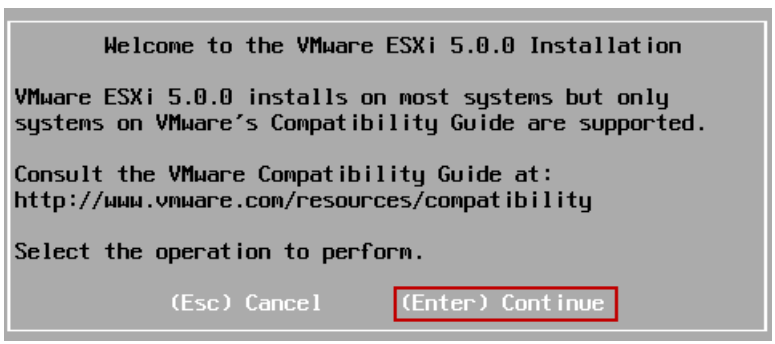
Welcome to the VMware ESXi 5.0.0 Installation
VMware ESXi 5.0.0 installs on most systems but only
systems on VMware's Compatibility Guide are supported.
Consult the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility
Select the operation to perform.
(Esc) Cancel
(Enter) Continue

Figure 8. Installation Welcome Screen

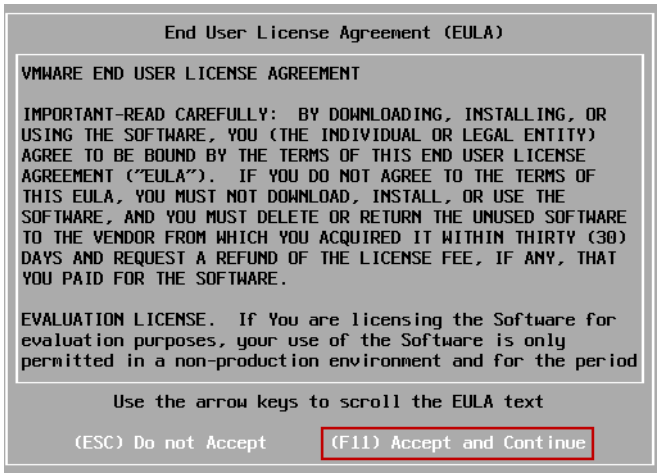
End User License Agreement (EULA)
VMWARE END USER LICENSE AGREEMENT
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.
EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period
Use the arrow keys to scroll the EULA text
(ESC) Do not Accept
(F11) Accept and Continue

Figure 9. End User License Agreement

4. Select the Local Storage Device to install ESXi. This can be a USB disk. Use the up and down arrow keys to select the device and press **Enter** (Figure 10)**.**

If a warning message that the device contents will be deleted, think again if there is any data on the storage device that will be lost. If there is, cancel the installation and move the data from the server.

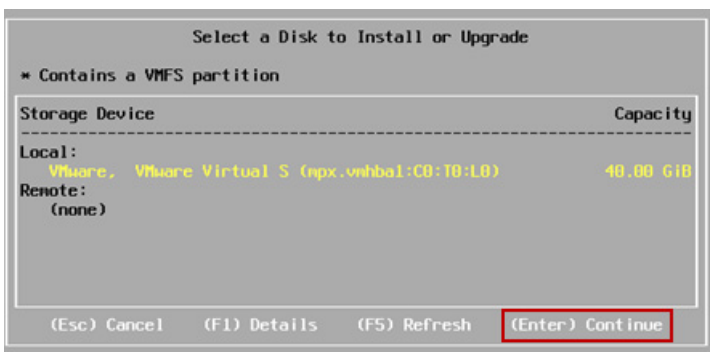

Figure 10. Selecting the Installation Destination

5. Using the up and down arrow keys to select the keyboard layout and press **Enter** (Figure 11).

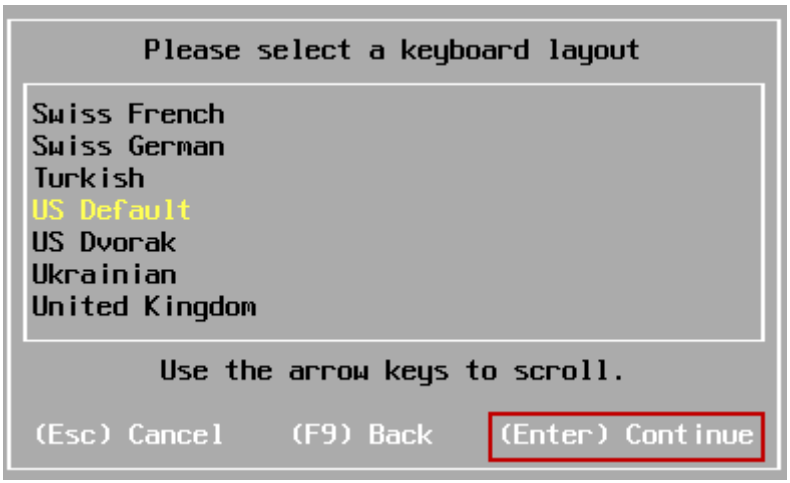

Figure 11. Keyboard Layout Selection

6. Enter the **Root password** (administrator) and confirm. Press **Enter** to continue (Figure 12).

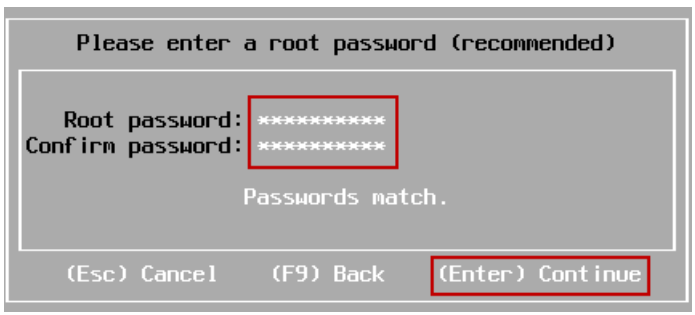

Figure 12. Enter Root Password

7. Confirm that the installation should commence by pressing **F11** (Figure 13).

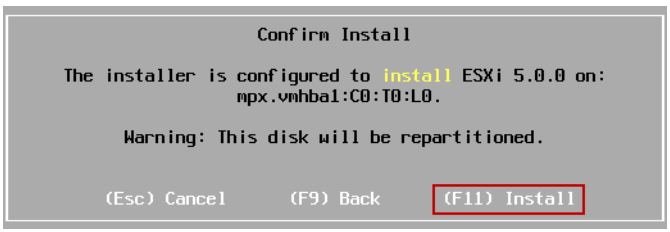

Figure 13. Confirming the Installation

8. When the installation is complete, remove the installation CD and press **Enter**. Wait until the VMware ESX server has finished booting (Figure 14).

Start customization to setup the management network address.

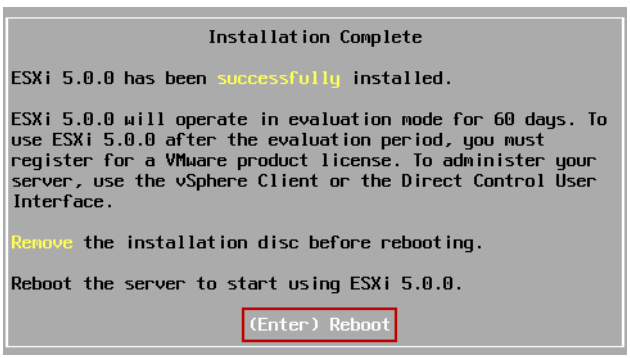
Installation Complete
ESXi 5.0.0 has been successfully installed.
ESXi 5.0.0 will operate in evaluation mode for 60 days. To use ESXi 5.0.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.
Remove the installation disc before rebooting.
Reboot the server to start using ESXi 5.0.0.
(Enter) Reboot

Figure 14. Installation Complete

9. Press **F2** to start customizing the server (Figure 15).
10. Configure the management network.
    a. Enter the root password and press **Enter**.
    b. Using the up and down arrow keys to select *Configure Management Network* and press **Enter**.
    c. Select *IP Configuration*, and press **Enter**.

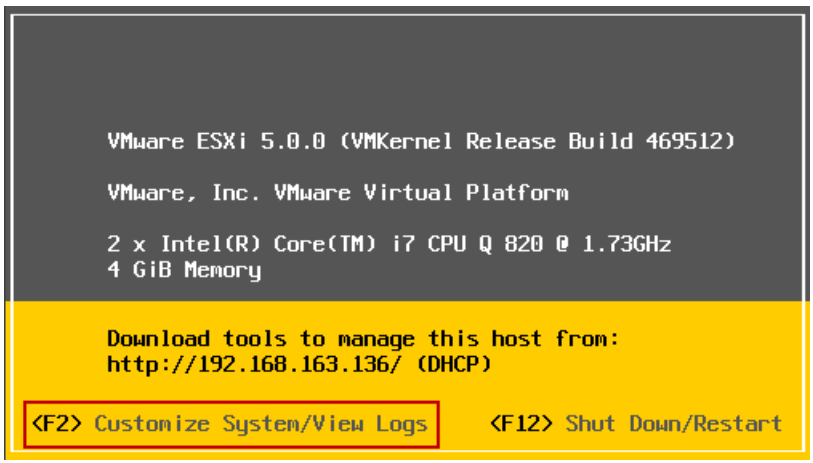
VMware ESXi 5.0.0 (VMKernel Release Build 469512)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Core(TM) i7 CPU Q 820 @ 1.73GHz
4 GiB Memory
Download tools to manage this host from:
http://192.168.163.136/ (DHCP)
<F2> Customize System/View Logs
<F12> Shut Down/Restart

Figure 15. Customize the Server

d. Select *Set static IP address and network configuration* by pressing the down arrow and then the space bar (Figure 16).

e. Use the down arrow on the keyboard to select the IP Address setting. Enter the IP Address, and Subnet Mask.
Set the Default Gateway to the same IP address as the ESXi server (Figure 16).

f. Press **Enter** to accept the values.

g. Press **Esc** to exit the configuration menu.

h. Press **Y** to apply the changes.

i. Press **Esc** to Log Out (Figure 17).

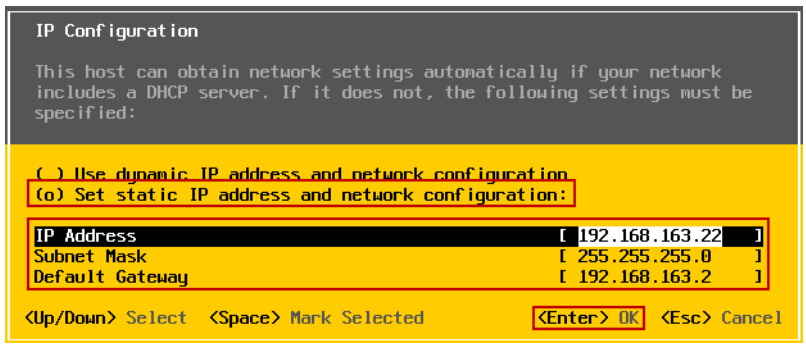
IP Configuration
This host can obtain network settings automatically if your network includes a DHCP server. If it does not, the following settings must be specified:
( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:
IP Address [192.168.163.22]
Subnet Mask [255.255.255.0]
Default Gateway [192.168.163.2]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

Figure 16. IP Configuration

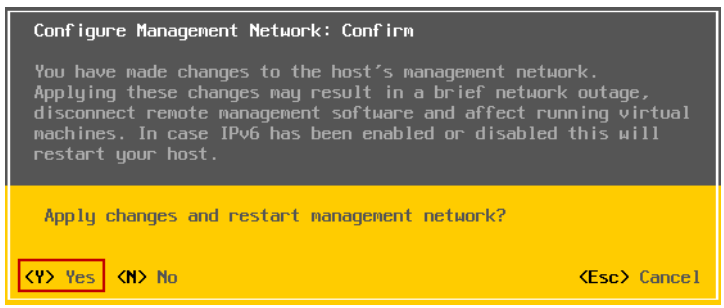
Configure Management Network: Confirm
You have made changes to the host's management network. Applying these changes may result in a brief network outage, disconnect remote management software and affect running virtual machines. In case IPv6 has been enabled or disabled this will restart your host.
Apply changes and restart management network?
<Y> Yes <N> No <Esc> Cancel

Figure 17. Confirmation of Configuration

VMware ESX Server Installation

The vSphere Client must be downloaded for future installation on the ESX clients.

The VMware ESX server software is not installed like a Windows application on top of Windows, but like an operating system directly on the computer. This means that ESX owns the hardware and no other operating system can be installed directly onto it in parallel.

A new installation of VMware ESX server software erases any existing data and removes existing partitions on the computer.

The VMware ESX 4.1 installation DVD is required for the installation. After purchasing an ESX license and registering on VMware's site, the user can download the ESX iso image which can then be burnt to a DVD.

Before installing ESX, start the computer and enter the BIOS. Enable “Execute Disable”, and “Virtualization VT”.

Ensure that an Ethernet cable is connected between the NIC that will be used to manage the ESX server and the physical network. To make it easier to identify this connection during installation of the ESX server, temporarily disconnect all other NICs on the ESX server. Once the ESX server is installed, connect the NICs again.

Perform the following to install VMware ESX server software:

1. Boot the computer from the VMware ESX server installation DVD to start the VMware ESX installer.
2. Click **Enter** to *Install ESX in graphical mode*.
3. From the *Welcome to the ESX Installer* window, click **Next**.
4. Read and accept the *End User License Agreement*, then click **Next**.
5. Select the keyboard and click **Next**.
6. Leave the *Custom Drivers* selected as *No* and click **Next**.
7. At the *Load Drivers*, *Load the system drivers* dialog, click **Yes**.
8. When *Load Drivers*, is complete, click **Next**.
9. Enter the serial number received from VMware and click **Next**.
10. Select the Network Adapter that will be used to manage the ESX Server which will have a green circle with white tick inside. Click **Next**.
11. Configure the following options from the Network Configuration window:
    a. Select *Use the following network settings:*
    b. Enter the IP address of the server (Format is: 192.168.128.xxx) with the subnet mask of 255.255.255.0.

The Gateway is required. If no gateway exists, use the same IP address as the ESX server is given in step 11.b.

Leave the DNS addresses blank unless DNS servers for the ESX servers are available. Enter a Host name for the VMware ESX. Ensure the host name is in the following format: <esx server name>.localdomain.local For example: (ESXSERVER1.localdomain.local).

c. Click **Next** when finished.

12. Setup type should be *Standard setup*. Click **Next**.
13. ESX Storage device should be the first hard disk. It is not supported to install ESX onto a USB device. Click **Next**.
14. A warning message that the device contents will be deleted will be displayed. Verify again if there is any data on the storage device that will be lost. If there is, cancel the installation and move the data from the server. If it is OK to delete the contents of the selected storage device, click **Next.**
15. From the Time Zone Settings, select a time zone and click **Next**.
16. For the Date and Time, leave the setting to manual, set the correct data and time, and click **Next**.
17. Set the root password, confirm password and click **Next**. The root user and password is used later to log on to the VMware ESX server. Remember the password.
18. Review the Summary of installation settings and click **Next**.
19. When the installation is complete, remove the installation DVD and click **Finish** to reboot the computer. Wait until the VMware ESX server has finished booting.

VMware ESXi 4.1 Server Installation

The VMware ESXi server software is not installed like a Windows application on top of Windows, but like an operating system directly on the computer. This means that ESXi owns the hardware and no other operating system can be installed directly onto it in parallel.

A new installation of VMware ESXi server software erases any existing data and removes existing partitions on the computer.

The VMware ESXi 4.1 installation CD is required for the installation.

This can be downloaded from VMware's site:
https://www.vmware.com/tryvmware/index.php?p=free-esxi&lp=1

The user needs to either login with an existing account, or create an account. The download page provides iso install CD images of ESXi that has customizations for either Dell, HP, or IBM. Download the iso that applies to the server, and burn it to a CD.

Before installing ESXi, start the computer and enter the BIOS. Enable “Execute Disable”, and “Virtualization VT”.

Ensure that an Ethernet cable is connected between the NIC that will be used to manage the ESX server and the physical network. To make it easier to identify this connection during installation of the ESXi server, temporarily disconnect all other NICs on the ESXi server. Once the ESXi server is installed, connect the NICs again.

VMware ESXi 4.1 supports SNMP when licensed with vSphere Essentials, vSphere Essential Plus, vSphere Standard, vSphere Advanced, vSphere Enterprise, or vSphere Enterprise Plus.

The free vSphere Hypervisor edition does not support SNMP.

For more details, refer to the VMware site:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1023990

Perform the following to install VMware ESXi server software:

1. Boot the computer from the VMware ESXi server installation CD to start the VMware ESXi installer. The installation is not a graphical interface.

2. The ESXi installation will automatically start a few seconds after the VMware installation screen is displayed.
3. From the *Welcome to the VMware ESXi 4.1* Installer window, press **Enter** to Install.
4. Read the *End User License Agreement*, then click press **F11** to accept and continue.
5. Select the disk where ESXi shall be installed to. This can be a USB disk. Use the up and down arrow keys to select the device and press **Enter.**

If a warning message that the device contents will be deleted, think again if there is any data on the storage device that will be lost. If there is, cancel the installation and move the data from the server.

6. Confirm that the installation should commence by pressing **F11**.
7. When the installation is complete, remove the installation CD and press **Enter**. Wait until the VMware ESX server has finished booting.

Two customizations must be made before using the ESXi server. They are to set the root password and the IP address for the ESXi server.

8. Press **F2** to start customizing the server.
9. Configure the root password.
    a. Using the up and down arrow keys on the keyboard, select *Configure Password* and press **Enter**.
    b. Enter the *New Password* and *Confirm Password*, and press **Enter**.
10. Configure the management network.
    a. Using the up and down arrow keys on the keyboard, select *Configure Management Network* and press **Enter**.
    b. Select *IP Configuration*, and press **Enter**.
    c. Select *Set static IP address and network configuration* by pressing the down arrow and then the space bar.
    d. Use the down arrow on the keyboard to select the IP Address setting. Enter the IP Address, and Subnet Mask. Set the Default Gateway to the same IP address as the ESXi server.

e. Press **Enter** to accept the values.

f. Select DNS Configuration.

g. Leave the DNS addresses blank unless DNS servers for the ESXi servers are available. Enter a Host name for the VMware ESX. Ensure the host name is in the following format: <esx server name>.localdomain.local For example: (ESXSERVER1.localdomain.local).

h. Press **Esc** to exit the DNS configuration menu.

i. Press **Esc** to exit the configuration menu.

j. Press **Y** to apply the changes.

k. Press **Esc** to Log Out.

vSphere Client Installation

vSphere Client is a separate client application used for configuring the VMware ESX(i) server (for creating VMs or changing their virtual hardware). The vSphere Client is required to be installed on at least one physical node, preferably an Engineering Client.

Always use the vSphere Client as the primary configuration tool where possible to configure VMware ESX servers. Do not make manual changes directly to the VMware ESX(i) configuration files through the Linux-based VMware ESX(i) Service Console.

Perform the following to install vSphere Client software:

1. Download the VMware vSphere Client from VMware.

For each version of ESX(i) make sure to install the same version of the vSphere Client. Multiple version can exist on the client.

Microsoft Windows operating system must already be installed on the Client node and the Client node has to have a physical network connection to the VMware ESX(i) server as described in Step 10 of Section 4, Installation and Configuration.

2. Transfer the vSphere Client to the Windows Client.

3. Run the vSphere Client installation program and use default settings.

4. Start the vSphere Client application by selecting the following:

   Start > Programs > VMware > VMware vSphere Client

5. Enter the VMware ESX(i) server IP address.
6. Enter **root** as user name and enter the password for the VMware ESX server that was chosen during installation.

When accessing the VMware ESX(i) server via the vSphere Client software, a warning about the VMware ESX(i) server's security certificate is displayed. The vSphere Client communicates with the VMware ESX(i) server via an SSL secured network connection using an SSL certificate which was automatically created on the VMware ESX(i) server during the VMware ESX(i) installation process. The self-signed default certificate is not recognized as a trusted certificate because it is not signed by a commercial Certification Authority (CA).

Self-signed certificates are vulnerable to man-in-the-middle attacks and clients receive a warning about them. Refer to the *VMware vSphere 4.1 Security Hardening Guide* (www.vmware.com/files/pdf/techpaper/VMware_vSphere_HardeningGuide_May10_EN.pdf) instruction for more information. Therefore, install a CA-signed certificate on the VMware ESX server. Refer to the ESX Server 3 Configuration Guide (www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf) instruction (Authentication and User Management section) for more information.

Setting ESX(i) time

When a virtual machine is started, it initially takes the time from the ESX(i) server. If there is a time synchronization inside the guest, the time will then be updated by it's time source. If the ESX(i) server is not synchronized to a reliable time server, this will create a step change in the time in the guest node which could interfere with the applications running inside the guest. It is important that the VMware tools is not synchronizing time with the ESX(i) server. This is the default setting and should not be changed.

The ESX(i) server internal clock must be synchronized to a reliable NTP server. This NTP server must have the same time as the 800xA system. Configuring of the NTP client in the ESX(i) server is performed through the vSphere Client.

1. Logon to the ESX(i) server, select **Configuration > Time Configuration > Properties**....
2. Press the **Options..** button.
3. In the options dialog, select NTP settings. Add the NTP server IP address using the **Add..** button.
4. Start the client using the **Start** button in the NTP Daemon Options dialog.
5. Close the dialog windows.
6. Confirm that the time is updated by selecting the Configuration tab and the Time Configuration option.

Set Up 800xA Server Nodes as VMs

This section details in the following topics:

- Create Virtual Switches on page 44.
- Create VMs and Connect them to Virtual Switches on page 46.
- Install 800xA into the VMs on page 47.

Create Virtual Switches

Prior to setting up VMs, it is good practice to setup the virtual network in which the VMs should run, using virtual switches. A virtual switch is an emulation of a physical switch. In VMware ESX(i), it is possible to create virtual switches and to connect VMs to these virtual switches to form a virtual network.

Perform the following to view and configure the virtual network of a VMware ESX(i) server:

1. Log on to the VMware ESX(i) server via the vSphere Client.
2. From the tree view on the left of the vSphere Client window, select the VMware ESX(i) server.
3. Select the Configuration tab and then select Networking.

Figure 18 shows an example of two virtual switches plant network 1 (PN1) and a control network 1 for area 20 (CN1 A20) to which different VMs are connected.

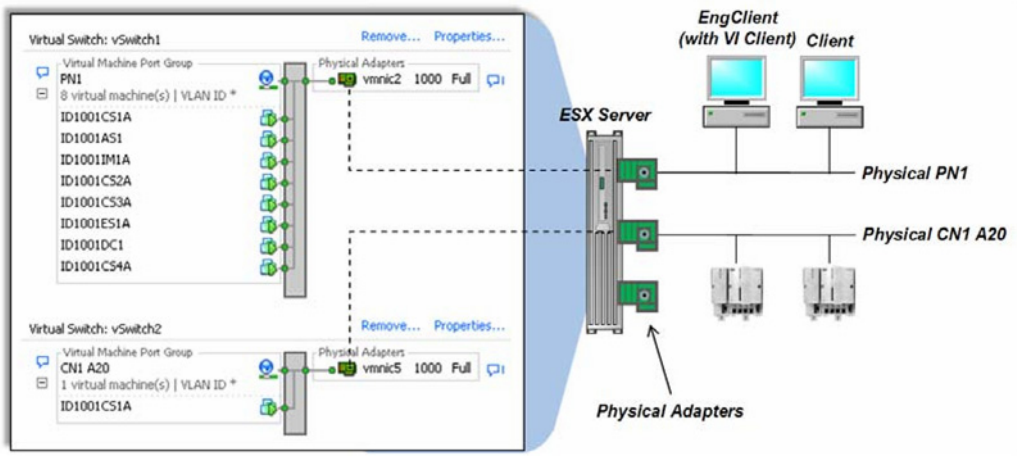

Figure 18. Virtual Network Configuration

A virtual switch can be bridged to a physical network adapter of the VMware ESX(i) server. This is shown in Figure 18 by the dotted lines. The VMware ESX(i) server itself is connected to the physical plant and control networks via these physical adapters. By doing so, virtual switches provide a means for connecting virtual 800xA server nodes to the physical system networks.

From VMware ESX(i) version 4.0, each VM can have a maximum of ten virtual network adapters. Therefore, a VM can be connected to a maximum of ten virtual switches. In the example of Figure 18, the virtual CS ID1001CS1A is connected to the plant network PN1 and to the control network CN1 A20. In the same manner, create a separate virtual switch for each physical plant or control network to which virtual 800xA server nodes require a connection. It is good practice to name a virtual switch like the physical network it is bridged to (for example, PN1 for the virtual switch bridged to the Physical PN1 as shown in Figure 18). For network redundancy, create a second virtual switch (for example, named PN2).

Perform the following to create a virtual switch:

1. From the Networking overview of the vSphere Client, select **Add Networking**. This opens the Add Network Wizard.
2. Select Virtual Machine as Connection Type and click **Next**.
3. Select an unclaimed physical adapter of the VMware ESX(i) server from the Create a virtual switch button and click **Next**.

Unclaimed means the physical adapter is not yet assigned to any other virtual switch.

4. From the Network Label field give the new virtual switch a meaningful name (for example, PN1) and click **Next**.
5. Click **Finish**.
6. To create additional virtual switches, repeat Step 1 through Step 5.

It is recommended to not connect the VMware ESX(i) Service Console with other VMs to the same virtual switch, but to use a separate virtual switch for the VMware ESX(i) Service Console.

Create VMs and Connect them to Virtual Switches

Perform the following to create VMs and connect them to virtual switches:

1. To create a VM, right-click on VMware ESX(i) server item and select **New Virtual Machine**. From the New Virtual Machine Wizard, specify the virtual hardware components and size of the VM such as virtual RAM or disk size.
2. Use Typical as Virtual Machine Configuration and click **Next**.
3. Give the VM a meaningful name (for example, PriAS) and click **Next**.
4. Select a datastore for the VM and click **Next**.

In VMware ESX(i), the physical disks of VMware ESX(i) servers are called datastores. To optimize disk performance, each VM should be stored on a separate datastore. The Domain Controller, which has lower disk access rates, can be stored on the same disk where the VMware ESX(i) server software is installed.

5. Select the operating system according to the requirements for the 800xA server node that is to be installed in the VM and click **Next**.

This does not actually install Windows inside the VM, but optimizes the VMs hardware to run the selected operating system. Installation of Windows and 800xA into the VM occurs later.

6. From the next two windows of the New Virtual Machine Wizard, select the proper CPU count and RAM size for the 800xA server node.
7. Select the number of virtual NICs for the 800xA server node and select which virtual switch (previously created) the NIC should be connected to. Ensure that the Connect At Power On option is selected for each NIC.
8. Select the virtual disk size for the 800xA server node and click **Next**.
9. Click **Finish**. In the left area of the vSphere Client window, the newly created virtual 800xA server node appears underneath the VMware ESX server tree view item.

The hardware configuration of the VM is viewed by the Summary tab of the VM and then selecting **Edit Settings**. Here, the user can add additional hardware to a VM as well as change existing hardware (such as increase the RAM size or completely remove hardware components).

10. To create additional VMs, repeat Step 1 through Step 9.

It is critical that all VMs virtual ethernet type is E1000.

Usage of a virtual ethernet adapter other than the E1000 type may cause loss of communication under certain conditions.

Install 800xA into the VMs

To install Windows, a Windows installation media from DVD or an ISO image is required. Each virtual 800xA node (each VM) requires its own Windows license. In this respect, a virtual installation does not differ from a physical installation.

Perform the following to make the installation media available to the VM:

1. Select a VM.
2. From the Summary tab, select **Edit Settings** to open the Virtual Machine Properties dialog.

3. Select the virtual CD/DVD drive of the VM. On the right of the dialog, select from options to mount a physical CD or to mount an ISO image. Ensure that Connect At Power On is selected.
4. Click **OK** to apply changes and close the dialog.
5. Boot the VM and start the Windows installation as follows:
   a. Select the Console tab to open a console to the VM.
   b. Start the VM by clicking the **Power On** button from the vSphere Client toolbar. This starts up the Windows installation in the Console tab.

After Windows is installed, install VMware Tools into the VM. The VMware Tools provide necessary drivers for the VM and further enhances its performance.

Perform the following to launch the VMware Tools installer:

1. From the vSphere Client menu, select:

   Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools

2. Ensure that the time synchronization option of the VMware Tools is disabled, to leave time synchronization control to 800xA.

After Windows and the VMware Tools are installed, install and configure 800xA software into the VM the same way as on physical computers by using the 800xA System Installer tool. For more information, refer to the *System 800xA Automated Installation (3BSE034679*)*.

The 800xA installation DVDs or ISO images can be mounted to the VM as described above. If the VM is connected to a physical network, it is also possible to

use Windows Explorer inside the VM to browse to the installation media located on a network share.

After installing the VMware tools, make sure to install the WDDM driver on the Virtual Machine running on either Windows 2008 R2 or Windows 7 Operating System.

Select **Control Panel > Device Manager** to install the WDDM driver.

On the hard disk, locate the drivers in the following path:

```
C:\Program Files\Common Files\VMware\Drivers\wddm_video\..
```

For more detailed instructions, refer to the documentation of Windows Operating System.

Section 5 Backup and Restore

This section describes the details of backup and restore activities performed in the ESX(i) server and in the virtual machines.

Backup and Restore of an ESX(i) Server

Backing up an ESX(i) server is a different concept to backing up a Windows computer.

Virtual machines running in an ESX(i) server are backed up individually as described in *Backup and restore of virtual machines*.

To install a replacement ESX(i) server as an assistance, the following configuration details should be noted:

- Virtual switch configuration. For example switch names, parameters, connected VMs.
- Storage adapter configuration. For example iSCSI addresses.
- NTP server details.
- DNS and routing configuration.
- User and Groups configuration.
- Virtual machine configuration such as resource allocation and user security details.

After the virtual machines have been moved to the new server, it is important to check that the network has been correctly set for each virtual machine.

When powering on a virtual machine which has been moved to the new server, a question may be asked if it has been copied or moved. Answering ‘moved’ will keep

the unique identity (for example NIC MAC addresses) the same. Answering ‘copied’ will change these unique identities.

Backup and Restore of Virtual Machines

Using snapshots is not a supported method for 800xA server nodes. There is a reduction in performance when running a virtual machine that has snapshots. If a snapshot has been made of a running virtual machine it can take longer to start the virtual machine. It is also possible to accidentally snapshot back to a previous state of the virtual machine which could interfere with production and potentially loose a great deal of data.

Virtual machines running in an ESX(i) server are backed up as if they are physical computers. The virtual machines are booted from an Acronis CD (in this case an ISO image that is uploaded to the ESX(i) Server), and the backup and restore made to a file server on the network.

Section 6 Security

When an ESX(i) server is installed, the root user is setup as the administrative user on all objects in the ESX(i) server. Items such as virtual machines that are added have the root user added to their permissions by default.

A danger with this is that mistakes or abuse of the system is possible by those who have knowledge of the root password. To limit this, additional users who have limited roles in the ESX(i) server should be added. These limited roles would only allow the user to start the virtual machine, but not stop, delete, or modify it. The roles should be applied to those virtual machines which are relevant to that user.

Roles

Roles are a group of privileges that can be allocated to a user and applied as permissions to the objects in the ESX(i) server. These privileges are grouped into categories such as Datastore and Virtual Machine.

By default, there are three roles in an ESX(i) server. These cannot be edited and new roles need to be created to define the required set of privileges.

Creating a role with a limited set of permissions through the following actions:

- Login to the ESX(i) Server using the **vSphere Client**.
- In the task bar, select **Home – Administration – Roles**.
- Select **Add Role**.
- Provide a name for the new role.
- By default, the new role has no privileges.
- Add the minimal level of privileges required.
  For example, expand the tree structure of:

All **Privileges – Virtual machine – Interaction**

Check the item: **Power On**.

- Select **OK**.

Users

Users are either those defined in the ESX(i) server, or via vCenter which uses Windows users. Once the users are defined, they are added to objects in the ESX(i) server and assigned permissions. When the user logs into the ESX(i) Server, only those virtual machines which have the user assigned to are visible.

Users are added through the following procedure:

- Login to the ESX(i) server using the vSphere Client.
- Select the ESX(i) server icon in the tree structure.
- Select the **Users & Groups** tab group.
- Right-click in the blank area in the **Users & Groups** tab.
- Select **Add...** from the context menu.
- Provide a Login, User Name and Password.
  The login name should have alphanumeric characters with no spaces. The password should meet the minimum complexity which is a minimum of 6-8 characters which have upper case, lower case, numeric values and do not contain phrases in the login name. If the password does not meet the minimum complexity, an invalid format message will be shown.

Permissions

Permissions are added to objects such as the virtual machines to allow users limited interaction with the virtual machine. They can be allowed to propagate to child objects.

Permissions are added to a virtual machine using the following procedure:

- Login to the ESX(i) server using the vSphere Client.
- Select the virtual machine which requires permission modification.
- Select the **Permissions** tab.
- Right-click in the blank area of the **Permissions** tab.
- Select **Add Permission...** from the context menu.
- Select **Add...** to select a user.
- Select the user name in the list.
- Press the **Add** button and then the **OK** button
- In the Assign Permissions window, select the permission from the Assigned Role drop down box.

If the ESX(i) server is being managed using vCenter Server, the users of the computer running vCenter Server, or the domain it is a member of, can be used to add permissions to the ESX(i) server objects.

Section 7 Optimizations

This section describes the optimizations required in virtual CPUs.

Virtual CPUs

As an initial guideline, it is recommended to have two virtual CPUs in each virtual machine and to have at least one logical processor per virtual CPU. In some cases, where there are a number of processes in the virtual machine which are consuming high processor load, it may be necessary to add additional virtual CPUs to achieve target performance levels.

To add an additional CPU to a virtual machine, it must first be shut down. The hardware configuration is then edited, and the number of CPUs adjusted to the required count. If a virtual machine has been configured with one processor, Windows will use the uniprocessor kernel. When more than one processor is found, Windows will then install the multiprocessor kernel and associated drivers. After this installation, the virtual machine needs to be restarted.

To provide CPU resources to the virtual machines, there should be one logical processor for each virtual CPU. For example, if the computer has 2 Quad Core CPUs (8 cores) and each virtual machine had 2 virtual CPUs, then there should be only 4 virtual machines running on the ESX(i) server (8 virtual CPUs).

Hyper threaded cores should not be counted as a single core since they share resources with the core and do not provide the equivalent performance of two cores.

Allocating Virtual CPUs to Physical Cores

It is highly recommended to allow the ESX(i) Server to allocate resources. However, if it is required to allocate virtual machine to physical cores, the identifier convention in the ESX(i) server must be understood.

In VMware ESX(i) server, the first hyper-thread of the first core is logical processor 0, the next hyper-thread of the first core is logical processor 1. This is summarized in Figure 19.

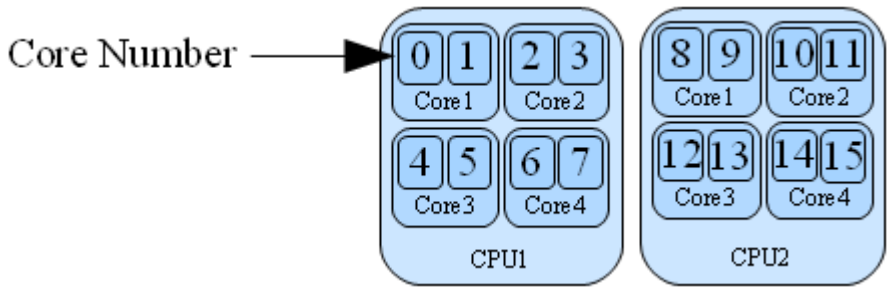

Figure 19. Core numbering in ESX

Section 8 Monitoring VMware vSphere ESX(i)

To ensure minimal disruption to production environments, it is important to monitor the ESX(i) server and be notified if an issue arises. To enable this functionality in ESX servers, a vendor specific management software is loaded into the ESX Server Console Operating System (COS). 800xA PNSM and AO communicate with the SNMP support provided by the management software to monitor the status of the server and notify the operator through the 800xA Alarm and Event system. The general procedure to setup monitoring is as follows:

1. Setup the network connections.
2. Install the required vendor management software on the ESX server.
3. Import the PNSM support into the 800xA Asset Optimization server.
4. Check that there is a Soft Alarm provider in the AO Server in the Event Collector group.
5. Create and configure the Aspect Object representing the ESX server.

This only applies to ESX not ESXi.

800xA 5.1 Rev B supports monitoring of ESXi 5.0 Servers. For more information, refer to Monitoring SNMP Traps in ESXi Server on page 82.

Setup the Network Connections

This section describes the setting up the network connections.

Supported Hardware for Virtualization

For more information on hardware that supports virtualization, refer to the following website:

http://inside.abb.com/product/se/9AAC171278.aspx?country=SE

Dell and HP Servers

To enable the 800xA AO server to monitor the ESX server, a network connection must be created between the AO server and the Service Console on the ESX server.

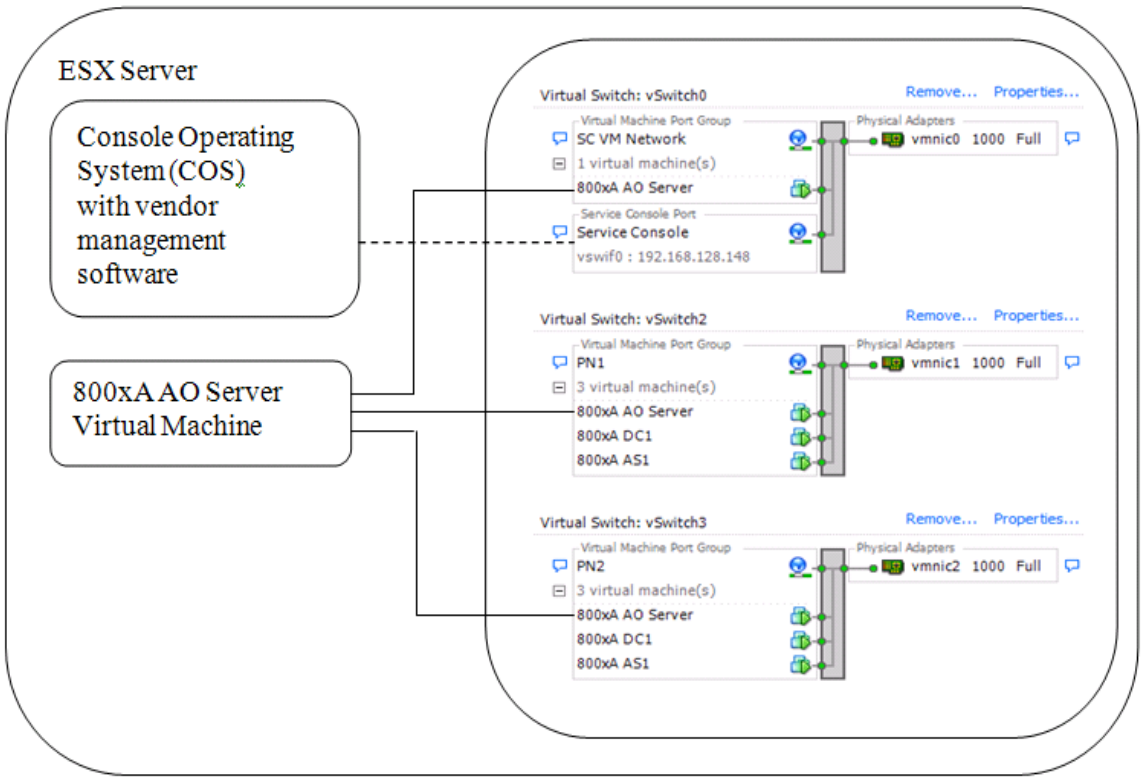

Figure 20. Example connection of AO server to ESX Service Console for PNSM & AO for Dell and HP servers

To configure the networking, perform the following actions:

1. Logon to the ESX server using the vSphere Client.
2. Review the network configuration and confirm that there is a Virtual Machine Port Group added to the vSwitch where the Service Console is attached. Add one if there is not one present.

3. Edit the AO server virtual machine.
4. Add a network adapter; setting it's virtual switch to the one connected to the Service Console. In the example, this would be **SC VM Network**.
5. Open a console to the AO virtual machine, configure the network adapter with an IP address on the same network as the Service Console.
6. Ping the address of the Service Console from the AO Server to confirm correct connection.

IBM Servers

IBM server differ from Dell and HP servers due to the SNMP support being provided by the inbuilt IMM module. This is available via dedicated network connection. To enable the 800xA AO server to monitor the ESX server, a network connection must be created between the AO server and the IMM module on the ESX server.

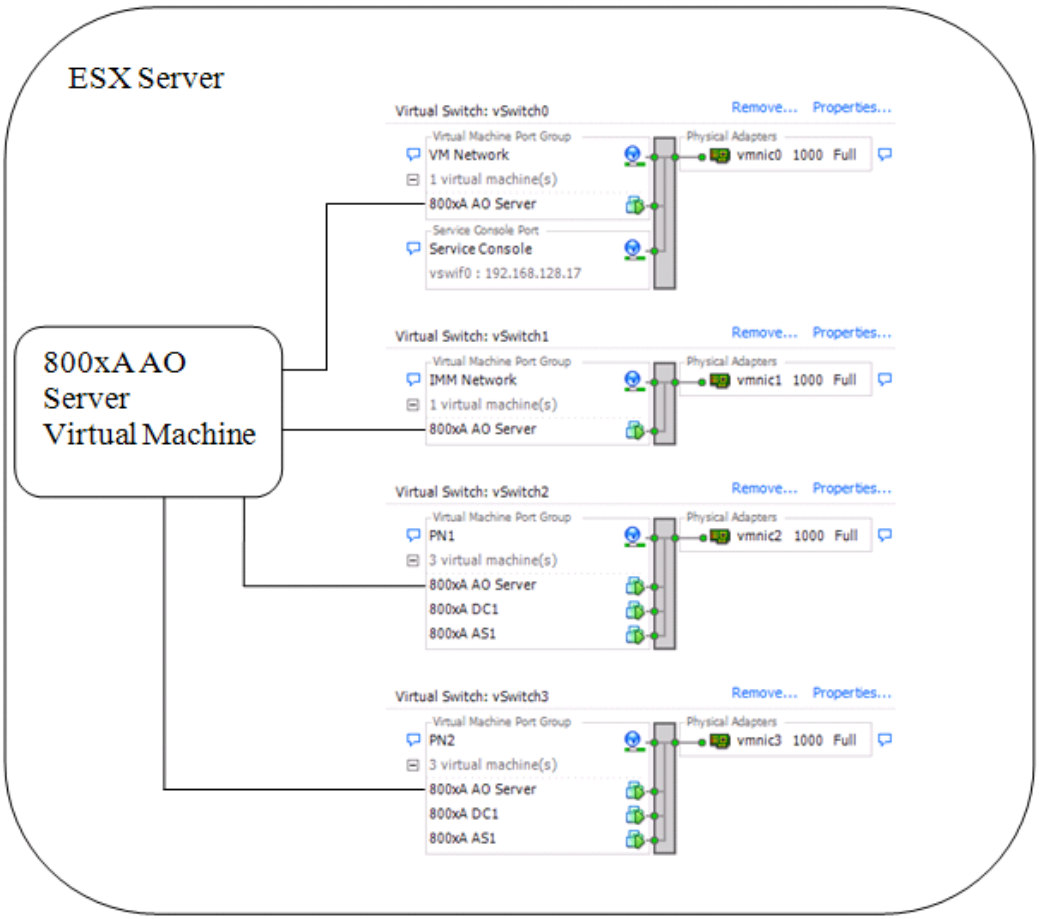

Figure 21. Example connection of AO server to ESX Service Console for PNSM & AO for IBM servers

To configure the networking, perform the following actions:

1. Logon to the ESX server using the vSphere Client.
2. Review the network configuration and confirm that there is a Virtual Machine Port Group added to the vSwitch where the IMM Module is connected and on to the Service Console networks. Add them if not already present.
3. Edit the AO server virtual machine.
4. Add networks adapter; setting their virtual switch to the one connected to the IMM and Service Console. In the example, this would be **VM Network** and **IMM Network** respectively.
5. Open a console to the AO virtual machine, configure the network adapters with an IP address on the same network as the Service Console and the IMM Module.
6. Ping the address of the Service Console and IMM Module from the AO Server to confirm correct connection.

Adding Vendor Management Software

Each vendor has its own management software that is installed into the ESX Server Console Operating System. This software is downloaded from the vendor's web site, and uploaded to the ESX server. Using the ESX terminal, the vendor software is then installed into the ESX server. The exception to this is the IBM Servers where the SNMP support is provided by the IMM Module.

Monitoring Dell R710 Running VMware vSphere ESX

The following describes the procedure to setup System 800xA to monitor a Dell R710 which is running VMware vSphere 4.1. It is assumed that VMware vSphere ESX 4.1 is installed on the Dell R710 server. A brief list of the pre-requisites is presented followed by the stepwise procedure for configuring the VMware vSphere ESX server and the System 800xA. Once the monitoring is configured, it is essential that it is tested in a non-destructive manner.

Pre-requisites

Hardware:

- Dell R710.

Software:

- VMware vSphere ESX 4.1.
- Dell OpenManage Server Administrator Managed Node.
- OM-SrvAdmin-Dell-Web-LX-6.4.0-1266.ESX41.i386_A00.2.tar.gz.
- System 800xA SV5.0 SP2 or higher with Asset Optimization server.
- 2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.
- 2PAA105767_B_en_DeviceObjectType_Dell_Poweredge_R710_V1_1_PNSM.

Procedure Summary

To setup System 800xA to monitor a Dell R710 which is running VMware vSphere 4.1 perform the following steps:

1. Configure networking of ESX and 800xA AO Server.
2. Install & Configure HP System Management in the ESX server.
3. Install & Configure 800xA PNSM Object types for R710.

Configure Networking of ESX and 800xA AO Server

Review the Setup Network Connections of this manual.

Installing Dell OpenManager Server Administrator Managed Node

1. Download the Dell OpenManager Server Administrator Managed Node software for VMware vSphere ESX 4.1 from the Dell Support website.
2. From the Dell website, select **Drivers & Downloads** - **Dell PowerEdge R710** - **ESX 4.1** - **System Management** - **Dell OpenManager Server Administrator Managed Node** (Distribution Specific)

   For example:

   OM-SrvAdmin-Dell-Web-LX-6.4.0-1266.ESX41.i386_A00.2.tar.gz

There are two possible files to download. One with the extension .sign, and other with extension .gz. Ensure that you are downloading the file with the .gz extension. This should be approximately 116MB.

3. Upload the file to one of the ESX Server datastores.
4. Logon to the ESX Server through the text based console as the root user.
5. Change directory to the datastore using the following command example:

   #cd /vmfs/volumes/datastore-name
6. Copy the OpenManager file to the root directory.

   #cp *.tar.gz /root
7. Change to root directory:

   #cd /root
8. Make directory for expanded files.

   #mkdir /root/dell
9. Expand file.

   #tar zxvf *.tar.gz -C dell
10. Change to dell directory.

    #cd /root/dell
11. Start Installation (in express mode).

    #sh setup.sh -x

12. Logout (paths needs to be updated).

    #exit

13. Logon to the ESX Server through the text based console.
14. Start services.

    #srvadmin-services.sh start

15. Open firewall.

    #/usr/sbin/esxcfg-firewall -o 1311,tcp,in,OpenManage

    #esxcfg-firewall -e snmpd

    #chkconfig snmpd on

    #service snmpd start

16. Logout.

    #exit

17. On a Windows client that is on the same network as the ESX server, open a web browser and use the following address: https://hostIP:1311

The hostIP is the IP address of the ESX server.

The System 800xA Asset Optimization Server must be able to ping this address.

Adding Support for Dell R710 to System 800xA

1. Copy the below mentioned files to the Aspect Optimization Server. Note that the DeviceObjectType_Base may already be present in the system.

   2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.exe

   2PAA105767_B_en_DeviceObjectType_Dell_Poweredge_R710_V1_1_PNSM.exe

2. Run the executable to extract the contents, and follow the instructions in the release notes file.

Configuration

1. Add an object of type Dell_Poweredge_R710_v1_1 under the IT OPC Server Network object as shown below:

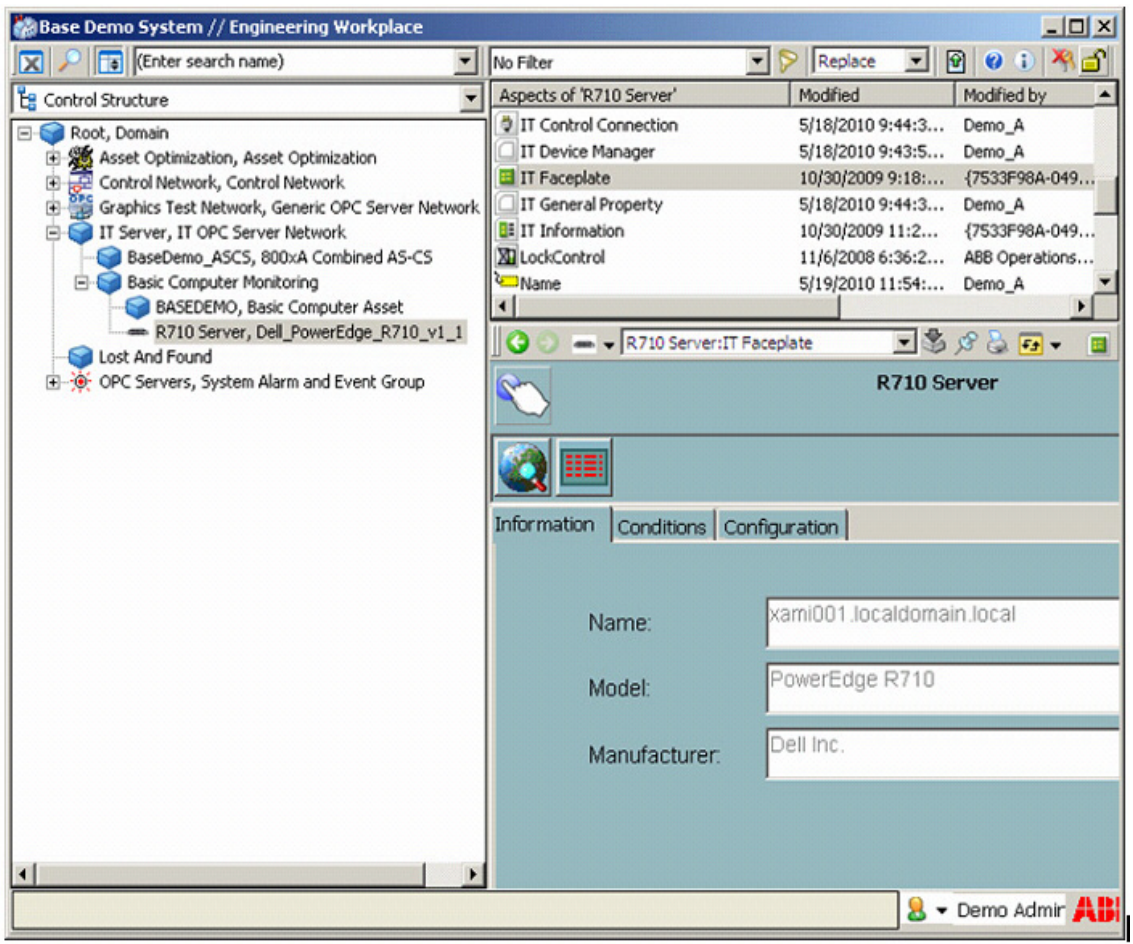

Figure 22. Dell R710 object

2. In the IT Faceplate aspect Configuration tab, set the IP address of the ESX server, and the SNMP community string as public.
3. Select the IT Device Manager and press the **Populate** button.

4. Enable alarms by executing the following:
   a. Select the **Alarm List - Config View**.
   b. Select **Open**.
   c. Expand the Condition Events.
   d. Enable Asset Optimization Alarms.
   e. Click **Apply**.
5. Load the configurations to the AO Server.
   a. Select the System Global Status object.
   b. Click **Load Configuration to AO Server**.
6. Select the Device Connection object.
   – Click **Load Configuration to AO Server**.

Confirmation: Test the Configuration

1. Select the Web Server aspect to login to the OpenManage interface. If a popup dialog box is shown requesting User Name and Password, click **Cancel**.
2. Select the IT Faceplate and confirm the server name and model.
3. Simulate a failure such as disconnecting one of the redundant power supplies. The alarm icon in the faceplate will indicate an error. Open the alarm list to see that the System General Condition is in alarm state. From the IT faceplate, select the WebServer button to logon to the OpenManage interface and view the cause of the error. Restore the power to the redundant supply and acknowledge the alarm.

Monitoring HP DL380 G6 Running VMware vSphere ESX

The following describes the procedure to setup System 800xA to monitor a HP DL380 G6 which is running VMware vSphere 4.1. It is assumed that VMware vSphere ESX 4.1 is installed on the HP DL380 G6 server. A brief list of the pre-requisites is presented followed by the stepwise procedure for configuring the VMware vSphere ESX server and the System 800xA. Once the monitoring is configured, it is essential that it is tested in a non-destructive manner.

Pre-requisites

- HP DL380 G6.
- VMware vSphere ESX 4.1 (ESXi is not supported).
- HP System Management Software for DL380G6.
- System 800xA SV5.0 SP2 or higher with Asset Optimization server.
- 2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.
- 2PAA105564_C_en_DeviceObjectType_HP_Proliant_DL380_G6_V1_2_PNSM.

Procedure Summary

1. Configure networking of ESX and 800xA AO Server.
2. Install & Configure HP System Management in the ESX server.
3. Install & Configure 800xA PNSM Object types for DL380G6.

Configure Networking of ESX and 800xA AO Server

Review the Setup Network Connections of this manual.

Install and Configure HP System Management in the ESX Server

HP provides the support for monitoring of the DL380 G6 running as an ESX Server. The supporting files need to be downloaded from the HP web site, transferred to the ESX Server and installed. This provides access to a management interface via a web browser.

The installation requires reboot at the end. All virtual machines on the server must be shutdown. Always do this from inside the virtual machine using the Start - Shutdown

1. Download the System Management software from the HP web site:
   a. Browse the internet to: www.hp.com
   b. Navigate/Search for: HP DL380 G6 - Drivers - ESX 4.1 - System Management.
   c. Download HP Management Agents for VMware ESX 4.x

      An example of the file name is: hpmgmt-8.6.0a-vmware4x.tgz
2. Logon to the ESX Server using the vSphere Client.
3. Upload the HP System Management File to a datastore. In the following example, the datastore was called Storage0.
4. Logon to the console of the ESX server (Alt-F1) using the root user.
5. Change directory to the datastore:

   #cd /vmfs/volumes/Storage0
6. Copy the file from the datastore to the root folder using the following command example:

   #cp hpmgmt-8.6.0a-vmware4x.tgz /root
7. Change back to the root folder:

   #cd /root
8. Extract the files using the following command:

   #tar zxvf hpmgmt-8.6.0a-vmware4x.tgz
9. Change directory to the installation folder:

   #cd hpmgmt/860a/
10. The ESX server must be placed into maintenance mode which means that all virtual machines must be either moved to another ESX server or shutdown.
11. Start the installation program.

#sh install860avibs.sh --install

In the following installation sequence, the address used for the AO server is 192.168.128.10 and a SNMP trap server of 192.168.128.2. SNMP trap servers receive SNMP trap notifications from devices and is an optional method for monitoring hardware. Refer to Monitoring SNMP Traps in ESXi Server on page 82.

Installation Sequence

This script will now attempt to set ESX Host in Maintenance Mode for IM agents install.

[root@ITC061 860a]# sh install860avibs.sh --install

Introduction message

```
HP Insight Manager Agent 8.6.0a-01 Installer for VMware ESX
 Target System is VMware ESX 4.1.0 build-260247
 Server: ProLiant DL380 G7
This script will now attempt to set ESX Host in Maintenance Mode for IM agents install.
Do you wish to continue? (y/n) y
```

If the ESX server is not in maintenance mode, the script will attempt to put the server into maintenance mode. Note that all the guests must be shut down.

```
Putting system into maintenance mode
ESX host Maintenance Mode is SET.
Installing HP Insight Manager Agents bulletin [classic-mgmt-solution-860a.01.1242]
....OK
```

```
/opt/hp/hp-agents-config ~/hpmgmt/860a
For accessing the System Management Homepage, the port for hpim service (2381)
should be enabled in the firewall.
Do you want to enable this port? <y/n> (default is y) y
Enabling port for hpim service (2381) in the firewall                [ OK ]
```

```
For allowing discovery by HP System Insight Manager, the port (2301)
should be enabled in the firewall.
Do you want to enable this port? <y/n> (default is y) y
Enabling port for HP System Insight Manager (2301) in the firewall       [ OK ]
```

```
For the Insight Manager agents to communicate properly with HP Systems Insight
Manager, the snmpd service should be enabled in the firewall.
Do you want to enable the snmpd service? <y/n> (default is y) y
Enabling snmpd service in the firewall                               [ OK ]
```

```
HP Advanced Server Management configuration:
This configuration script will configure SNMP to integrate with the HP SIM and
the HP System Management Homepage by editing the snmpd.conf file. The HP-
SNMP-Agents can also exist in a more secure
SNMP environment (e.g. VACM) that you have previously configured. See the
hp-snmp-agents(4) man page for specific details on how to configure the VACM
entries
in the 'snmpd.conf' file. You may press <Ctrl+c> now to exit now if needed.
Do you wish to use an existing snmpd.conf (y/n) (Blank is n): n
```

You will now be asked a series of SNMP configuration questions. How you answer these question will affect the way SNMP behaves. Configuring SNMP could have security implications on your system. If you are not sure how to answer a question, you can abort by pressing <Ctrl-c> and no changes will be made to your SNMP configuration. Enter the localhost SNMP Read/Write community string (one word, required, no default): Re-enter the same input to confirm:
ACCEPTED: inputs match!
Enter localhost SNMP Read Only community string (one word, Blank to skip): Re-enter the same input to confirm: ACCEPTED: inputs match!

The address entered for the Authorization Management Station is the IP address of the AO server.

Enter Read/Write Authorized Management Station IP or DNS name (Blank to skip): 192.168.128.10
Enter SNMP Read/Write community string for Management Station "192.168.128.10" (one word, required, no default): Re-enter the same input to confirm: ACCEPTED: inputs match!
Enter Read Only Authorized Management Station IP or DNS name (Blank to skip): 192.168.128.61
Enter SNMP Read Only community string for Management Station "192.168.128.10" (one word, required, no default): Re-enter the same input to confirm: ACCEPTED: inputs match!

Enter default SNMP trap community string (One word; Blank to skip): public
Enter SNMP trap destination IP or DNS name (One word; Blank to skip): 192.168.128.10
Enter trap community string for trap destination "192.168.128.10" (One word; Blank to skip): public
The system contact is set to syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf) Do you wish to change it (y/n) (Blank is n): n

```
The system location is set to
syslocation Unknown (edit /etc/snmp/snmpd.conf)
Do you wish to change it (y/n) (Blank is n): n
============================================================
NOTE: New snmpd.conf entries were added to the top of /etc/snmp/snmpd.conf
============================================================
snmpd is started                                          [ OK ]
Stopping System Management Homepage:                    [ OK ]
Starting HP Insight Manager agents:                       [ OK ]
Starting System Management Homepage:                     [ OK ]
Stopping SNMP stack:
      Stopping snmpd:                                   [ OK ]
Starting SNMP stack:
      Starting snmpd:                                   [ OK ]
************************************************************
* System Management Homepage installed successfully with *
* default configuration values.   To change the default  *
* configuration values,  type the following command at   *
* the root prompt:                                       *
*                                                        *
* /opt/hp/hpsmh/sbin/smhconfig                           *
*                                                        *
************************************************************
Please read the License Agreement for this software at
/opt/hp/hp-health/hp-health.license
By not removing this package, you are accepting the terms
of the "License for HP Value Added Software".
HP Insight Manager agents have been configured successfully!
~/hpmgmt/860a
      HP SNMP agents are installed and configured
      Reboot the system to make the changes effective.
ESX host Maintenance Mode is UNSET.
ESX host Maintenance mode is reset to normal.
```

Reboot the ESX server using the reboot command.

1. When the ESX server has completed rebooting, start a web browser and go to the web page:

   https://youresxip:2381

Ensure that your proxy setting excludes the IP address of the ESX server You will need to accept the certificate from the server.

2. Logon using the root user account.
3. Never use the web browser remember password function.
4. Navigate to the Array Controller Information.

In this ESX server, the first disk has been temporarily been removed.

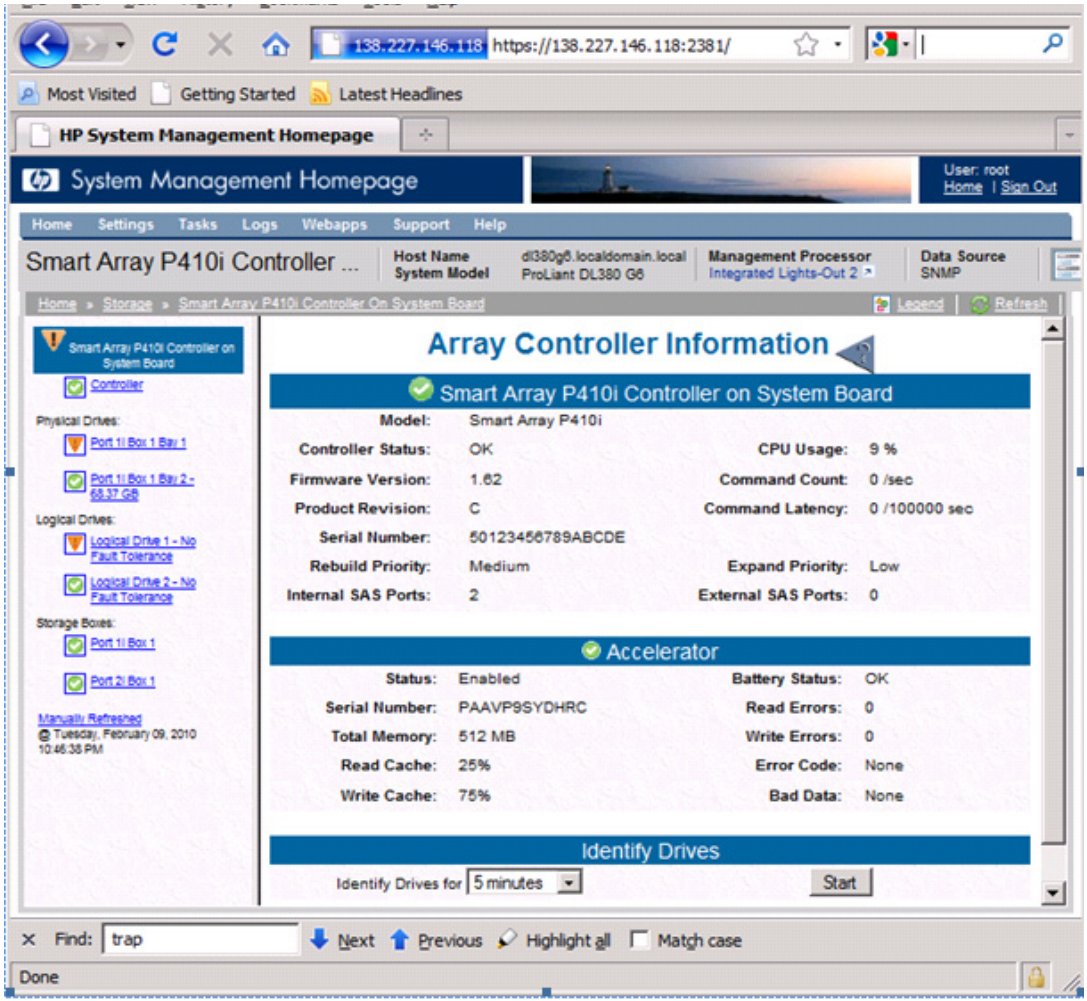

Figure 23. HP System management Homepage

Adding ABB Object Types

The object type should be unpacked separately in the Aspect Server, and the AO Server.

1. In the Aspect Server, the Object Type is imported.
2. In the AO Server, the script is run.

1. Add in latest base object.

For example: 2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.exe

   a. Double click on executable to unpack it.

   b. Import the Base_PNSM.

   c. Import the Alarm Control VB6 or PG2 based on PG2 availability.

   d. Run the install.bat

2. Add in the server object type.

For example:
2PAA105564_C_en_DeviceObjectType_HP_Proliant_DL380_G6_V1_2_PNSM.exe

   a. Double click on executable to unpack it.

   b. Import the 10_ object.

   c. Import the 11_ object for VB6 based systems, or 12_ for PG2 based systems.

Creating Objects

1. Add object to Control Structure for each of the ESX Servers.
2. Select

   a. Root, Domain

   b. Asset Optimization, Asset Optimization

   c. IT Server, ITOPC Server Network

   d. Basic Computer Monitoring

3. Right-click and Add new object.
4. Select server model. e.g. HP Proliant DL380 G6 V1_2.
5. Provide a Name.
6. In the IT Faceplate aspect, select the configuration tab enter the IP address, SNMP community and set the Controller Index to 0.

If the Controller Index is no set, the Drive Array Controller status may be incorrect

Configure the Object

1. Select the IT Device Manager aspect and press **Populate**.
2. On each of the following aspects, select the Config View, and Load the Configuration to the AO Sever:
   a. Memory System Board-1.
   b. Memory System Board-2.
   c. Device Connection.
   d. Drive Array Controller.
   e. Overall Thermal and Fan Status.
   f. Power Subsystem.
3. Select **Alarm list - Configure - Open**.
4. Select all categories.

Monitoring IBM x3650M2 Running VMware vSphere ESX

The following describes the procedure to setup System 800xA to monitor a IBM x3650M2 which is running VMware vSphere 4.1. It is assumed that VMware vSphere ESX 4.1 is installed on the IBM x3650M2 server. A brief list of the pre-requisites is presented followed by the stepwise procedure for configuring the VMware vSphere ESX server and the System 800xA. Once the monitoring is configured, it is essential that it is tested in a non-destructive manner.

Pre-requisites

- IBM x3650M2
- VMware vSphere ESX 4.1 (ESXi is not supported).
- System 800xA SV5.0 SP2 or higher with Asset Optimization server.
- 2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.
- 2PAA106214_A_en_DeviceObjectType_IBM_x3650_M2_V1_0_PNSM.

Procedure Summary

1. Configure networking of ESX and 800xA AO Server.
2. Install & Configure 800xA PNSM Object types for the IBM x3650M2.

Configure Networking of ESX and 800xA AO Server

Review the Setup Network Connections of this section of the manual

Configure the ESX Server

1. Logon to the ESX Server through the text based console.
2. Open firewall:

```
#esxcfg-firewall -e snmpd
#chkconfig snmpd on
#service snmpd start
#exit
```

Adding ABB Object Types

The object type should be unpacked separately in the Aspect Server, and the AO Server.

1. In the Aspect Server, the Object Type is imported.
2. In the AO Server, the script is run.

1. Add in latest base object.

   For example: 2PAA102558_J_en_DeviceObjectType_Base_V1_9_PNSM.exe
2. Double click on executable to unpack it.
3. Import the Base_PNSM.
4. Import the Alarm Control VB6 or PG2 based on PG2 availability.
5. Run the install.bat
6. Add in the server object type.

For example:
2PAA106214_A_en_DeviceObjectType_IBM_x3650_M2_V1_0_PNSM.exe

7. Double click on executable to unpack it.
8. Import the 10_ object.
9. Import the 11_ object for VB6 based systems, or 12_ for PG2 based systems.

Creating Objects

1. Add object to Control Structure for each of the ESX Servers.
2. Select
   a. Root, Domain
   b. IT Server, IT OPC Server Network
3. Right-click and Add New Object…
4. Select server model. e.g. IBM_x3650M2_v1_0.
5. Provide a Name for the object and press Create.

6. In the IT Faceplate aspect, select the Configuration tab enter the IP address of the server, the SNMP community string, and the IP address of the IMM Module.

Configure the Object

1. Select the IT Device Manager aspect and press **Populate**.
2. On each of the following aspects, select the Config View, and Load the Configuration to the AO Sever:
   a. Device Connection
   b. System Health Status
3. Select **Alarm list - Configure - Open.**
4. Select all categories.
5. Press **Apply**.

Monitoring SNMP Traps in ESXi Server

System 800xA supports virtualization for a physical server, running on VMware ESXi. ESXi is installed either on to the hard disk, SD card or USB stick. Many servers have facilities to mount these on circuit boards inside the chassis. ESXi does not support the service console (and does not support any management software) that is available in ESX. Therefore, monitoring ESXi server hardware using PC, Network and Software Monitoring (PNSM) server is not possible.

Similar to ESXi, SAN devices do not support installing additional SNMP management software. In order to monitor the ESXi server hardware and SAN devices in the System 800xA, SNMP trap support is now a feature of PNSM.

SNMP Trap is a message that is initiated by an IT Asset (agent) and sent to the network management system (manager). If an event has occurred, the agent communicates it to the manager using the Trap. Traps are sent asynchronously and not in response to the queries from the manager. The manager is responsible for

performing an action, based on the Trap it receives from the agent. SNMP trap messages are presented as alarms and events in System 800xA.

If the localhost is used then some servers identify themselves as 0.0.0.0, which prevents correct functionality of the ABB SNMP Trap support.

Configuring IT SNMP Trap Service

IT SNMP Trap Service is configured to monitor the ESXi server hardware and peripherals like SAN storage. The service is responsible for receiving the trap messages from IT devices and presenting these messages as alarms and events in the system.

Perform these steps to configure IT SNMP Trap Service.

In the Service Structure:

1. Right-click IT SNMP Trap Service.

   Creating Service Group:

   a. Select **New Object** and create Service Group.

   b. Enter the Service Group **Name**.

   Creating Service Provider:

   a. Right-click Service Group.

   b. Select **New Object** and create Service Provider.

   c. Enter the Service Provider **Name**.

2. Click **Service Provider Definition** in the Aspect list area.

3. Click **Configuration** and set the following (Figure 26):

   – Select the **Enabled** check box
   – Service needs to be in **Current** state
   – **Node** is set to the <Computer Name>

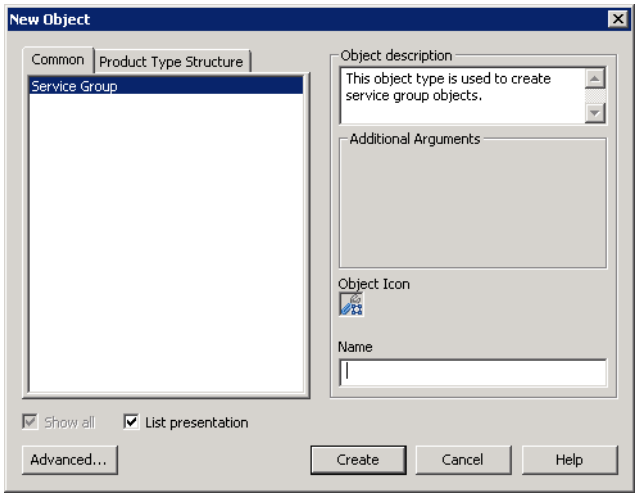

Figure 24. Creating Service Group

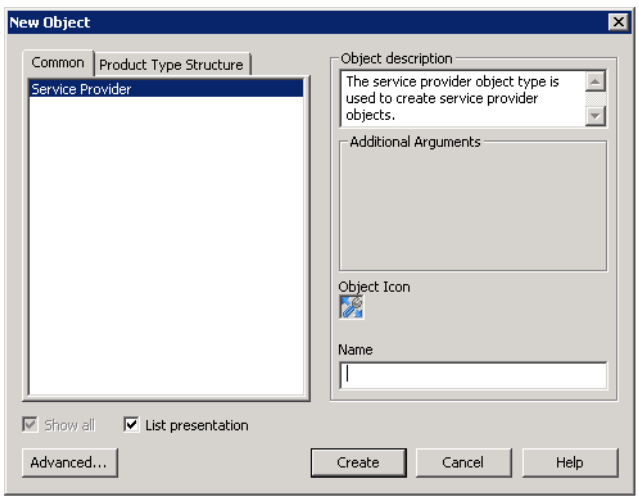

Figure 25. Creating Service Provider

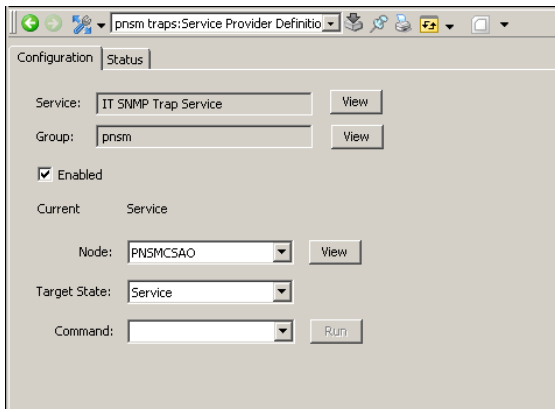

Figure 26. IT SNMP Trap Service Configuration

Configuration of IT SNMP Trap Service must be done on the PNSM server.

The following servers are supported for monitoring SNMP traps in 800xA.

- Dell R710
- IBM x3650 M2
- HP DL380 G6

For example:

Set up the Dell R710 server for SNMP Trap as follows:

1. Create an instance of the object type in **Control Structure** for server to be monitored.
2. In the IT Faceplate Aspect View, select **Configuration** and enter the IP Address.

Click the **Password** button to provide the password for SNMP community.

3. **IT Device Trap** aspect displays the list of server traps (Figure 27).
4. On the view selection drop-down , select **Config View** to change Message, Severity, and Notification.

5. Click **Deploy** to save the changes.
6. Select the IT Device Manager aspect and press **Populate**.

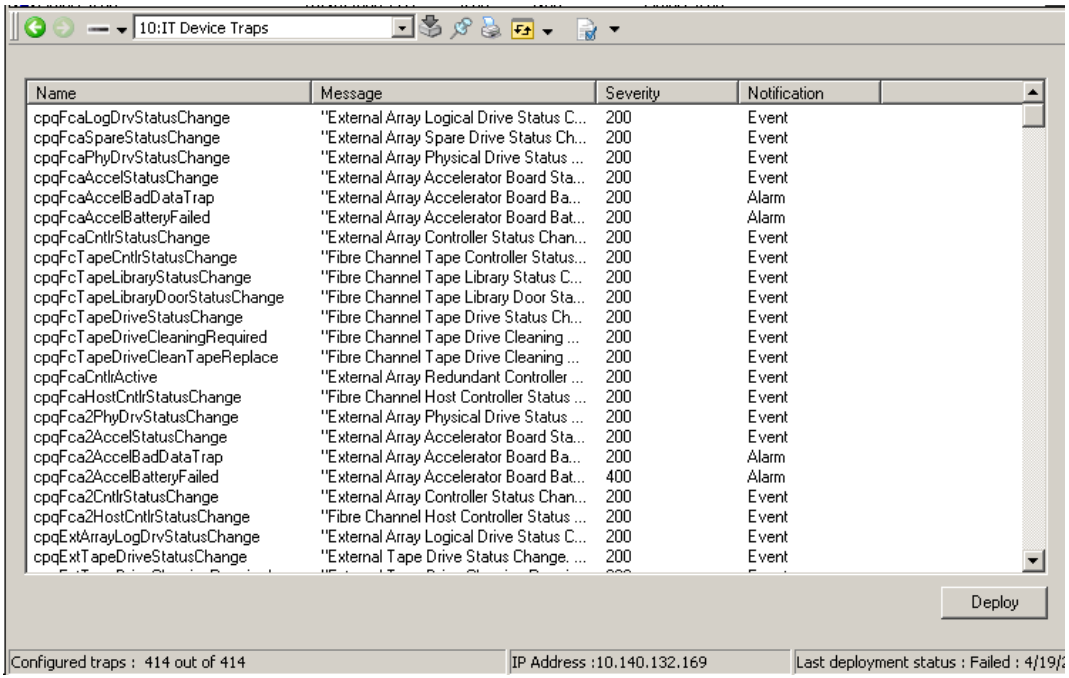
10:IT Device Traps
Name
Message
Severity
Notification
cpqFcaLogDrvStatusChange "External Array Logical Drive Status C... 200 Event
cpqFcaSpareStatusChange "External Array Spare Drive Status Ch... 200 Event
cpqFcaPhyDrvStatusChange "External Array Physical Drive Status ... 200 Event
cpqFcaAccelStatusChange "External Array Accelerator Board Sta... 200 Event
cpqFcaAccelBadDataTrap "External Array Accelerator Board Ba... 200 Alarm
cpqFcaAccelBatteryFailed "External Array Accelerator Board Bat... 200 Alarm
cpqFcaCntlrStatusChange "External Array Controller Status Chan... 200 Event
cpqFcTapeCntlrStatusChange "Fibre Channel Tape Controller Status... 200 Event
cpqFcTapeLibraryStatusChange "Fibre Channel Tape Library Status C... 200 Event
cpqFcTapeLibraryDoorStatusChange "Fibre Channel Tape Library Door Sta... 200 Event
cpqFcTapeDriveStatusChange "Fibre Channel Tape Drive Status Ch... 200 Event
cpqFcTapeDriveCleaningRequired "Fibre Channel Tape Drive Cleaning ... 200 Event
cpqFcTapeDriveCleanTapeReplace "Fibre Channel Tape Drive Cleaning ... 200 Event
cpqFcaCntlrActive "External Array Redundant Controller ... 200 Event
cpqFcaHostCntlrStatusChange "Fibre Channel Host Controller Status ... 200 Event
cpqFca2PhyDrvStatusChange "External Array Physical Drive Status ... 200 Event
cpqFca2AccelStatusChange "External Array Accelerator Board Sta... 200 Event
cpqFca2AccelBadDataTrap "External Array Accelerator Board Ba... 200 Alarm
cpqFca2AccelBatteryFailed "External Array Accelerator Board Bat... 400 Alarm
cpqFca2CntlrStatusChange "External Array Controller Status Chan... 200 Event
cpqFca2HostCntlrStatusChange "Fibre Channel Host Controller Status ... 200 Event
cpqExtArrayLogDrvStatusChange "External Array Logical Drive Status C... 200 Event
cpqExtTapeDriveStatusChange "External Tape Drive Status Change. ... 200 Event
Deploy
Configured traps : 414 out of 414
IP Address :10.140.132.169
Last deployment status : Failed : 4/19/

Figure 27. SNMP Trap from a Dell Server

Each of these traps consists off:

Table 1. Trap Configuration

Name	Description
Trap Name	Represents the name of the trap as seen in MIB file.
Message	Lists the corresponding Trap messages.

Table 1. Trap Configuration

Name	Description
Severity	Indicates the severity of the Traps. By default the value is 250. The value ranges between 1 -1000.
Notification	Indicates if the message is an alarm or an event.

Traps are represented as alarms and events in the System 800xA.

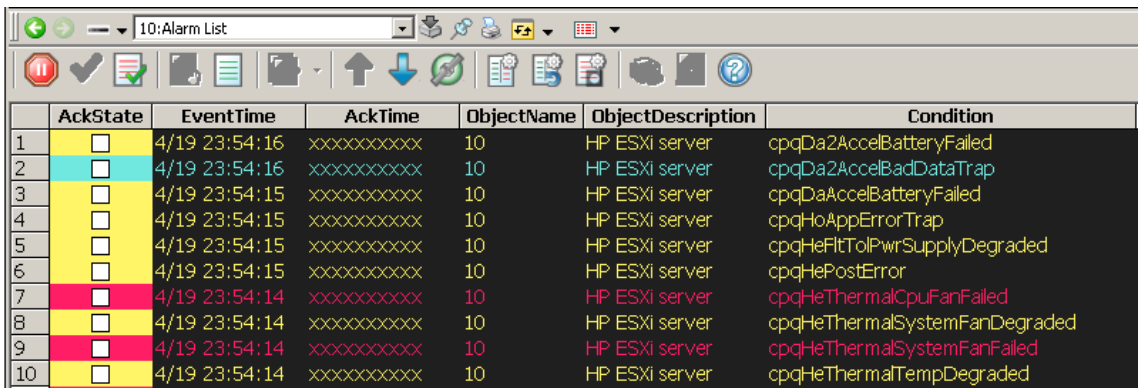
10:Alarm List
AckState
EventTime
AckTime
ObjectName
ObjectDescription
Condition
1 4/19 23:54:16 xxxxxxxxxx 10 HP ESXi server cpqDa2AccelBatteryFailed
2 4/19 23:54:16 xxxxxxxxxx 10 HP ESXi server cpqDa2AccelBadDataTrap
3 4/19 23:54:15 xxxxxxxxxx 10 HP ESXi server cpqDaAccelBatteryFailed
4 4/19 23:54:15 xxxxxxxxxx 10 HP ESXi server cpqHoAppErrorTrap
5 4/19 23:54:15 xxxxxxxxxx 10 HP ESXi server cpqHeFltTolPwrSupplyDegraded
6 4/19 23:54:15 xxxxxxxxxx 10 HP ESXi server cpqHePostError
7 4/19 23:54:14 xxxxxxxxxx 10 HP ESXi server cpqHeThermalCpuFanFailed
8 4/19 23:54:14 xxxxxxxxxx 10 HP ESXi server cpqHeThermalSystemFanDegraded
9 4/19 23:54:14 xxxxxxxxxx 10 HP ESXi server cpqHeThermalSystemFanFailed
10 4/19 23:54:14 xxxxxxxxxx 10 HP ESXi server cpqHeThermalTempDegraded

Figure 28. Alarms Traps

Traps are represented as events in the System 800xA.

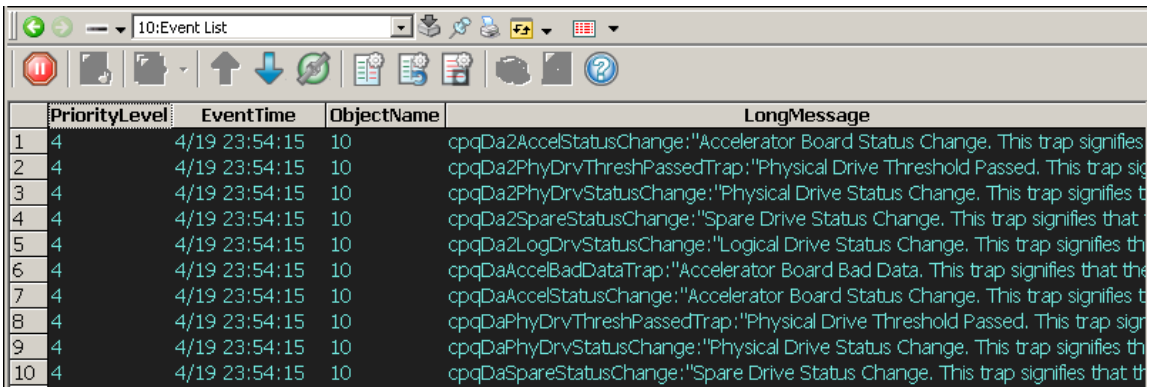
10:Event List
PriorityLevel EventTime ObjectName LongMessage
1 4 4/19 23:54:15 10 cpqDa2AccelStatusChange:"Accelerator Board Status Change. This trap signifies
2 4 4/19 23:54:15 10 cpqDa2PhyDrvThreshPassedTrap:"Physical Drive Threshold Passed. This trap sig
3 4 4/19 23:54:15 10 cpqDa2PhyDrvStatusChange:"Physical Drive Status Change. This trap signifies t
4 4 4/19 23:54:15 10 cpqDa2SpareStatusChange:"Spare Drive Status Change. This trap signifies that
5 4 4/19 23:54:15 10 cpqDa2LogDrvStatusChange:"Logical Drive Status Change. This trap signifies th
6 4 4/19 23:54:15 10 cpqDaAccelBadDataTrap:"Accelerator Board Bad Data. This trap signifies that the
7 4 4/19 23:54:15 10 cpqDaAccelStatusChange:"Accelerator Board Status Change. This trap signifies t
8 4 4/19 23:54:15 10 cpqDaPhyDrvThreshPassedTrap:"Physical Drive Threshold Passed. This trap sign
9 4 4/19 23:54:15 10 cpqDaPhyDrvStatusChange:"Physical Drive Status Change. This trap signifies th
10 4 4/19 23:54:15 10 cpqDaSpareStatusChange:"Spare Drive Status Change. This trap signifies that th

Figure 29. Event Traps

Configuring the Alarm and Event List

Configure the Alarm and Event from view configuration. The steps are as follows:

1. Click **View Configuration** .
2. Alarm and Event list configuration dialog box appears.
3. Choose the **Source** as **Alarms** and select **Categories** as shown in the Figure 30.
4. Choose the **Source** as **Events** and select **Categories** as shown in the Figure 31.

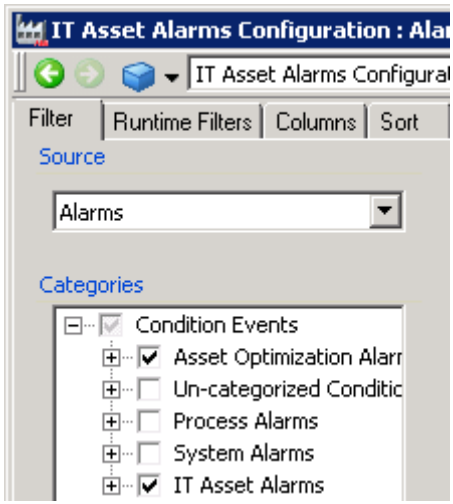

Figure 30. Alarm List Configuration

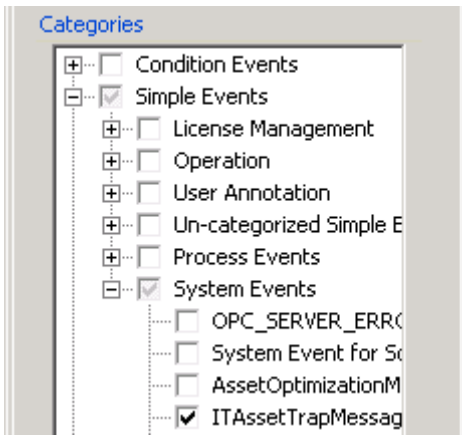

Figure 31. Event List Configuration

Section 9 Installing VMware CLI, Drivers, Updates and Upgrades

When setting up an ESX server, additional drivers may be required. Typically, this would be for network adapters. Additional updates may also be required. These tasks can be achieved from the Windows computer which is used as a client to the ESX server.

Additional software is required for this type of interaction with the ESX server. VMware has produced a software utility which provides the functionality to have patches that have been save on the Windows client be applied to the ESX server through simple commands. To make it easier to identify the update files when typing the commands, they should be placed in a simple folder such as C:\ESXUpdates

Most vendors produce iso images which are used to create bootable cds/dvds to enable the firmware to be upgraded.

VMware Command Line Interface

The VMware Command Line Interface (CLI) provides the ability to perform maintenance operations such as applying patches, drivers and updates from a Windows client. This removes the necessity to understand the Unix based command required when logging in via the text based terminal console for these tasks. It also provides the ability to apply updates to ESXi where there is no text based console to log in to.

Installing VMware Command Line Interface

VMware CLI is downloaded from VMware. While it is free to download, a VMware account to login to the VMware website is necessary.

1. To download the VMware CLI, go to www.vmware.com.
2. Select **Support & Downloads**.
3. Select **VMware vSphere**.
4. At the **Download VMware vSphere 4** web page, select **Drivers & Tools**.
5. Expand **Automation Tools and SDKs**.
6. If ESX 4.0 Update1 is being used, download **VMware vSphere CLI 4.0 U1**.
7. If ESX 4.1 is being used, download **VMware vSphere CLI**.
8. VMware will request login details if necessary.
9. You will need to accept the VMware End User License Agreement.
10. At the download page, select Download Options **Use Web Browser**.
11. Select the **exe** link for the **VMware vSphere Command - Line Inferface - Windows Installer**.
12. Save the installation file to the local disk.
13. Double click on the downloaded file to begin installation.
14. If a dialog box O**pen File - Security Warning** appears, press the **Run** button.
15. At the Welcome dialog, press **Next**.
16. At the License Agreement, select **I accept the terms in the license agreement**, Then, select **Next**.
17. At the Destination folder dialog, select **Next**.
18. At the Ready to Install dialog, select **Install**.
19. At the Installation Wizard Completed dialog, press **Finish**.

Installing Drivers

VMware CLI is a requirement for installing drivers.

Identify Hardware Requiring Additional Drivers

Due to the difficulty in identifying hardware which ESX does not automatically detect, it is vital to have an inventory of the computers configuration. This should contain details on, for example, additional NIC cards including the chipset. This information is used to identify the correct driver in the VMware web site.

Download Driver from VMware

The following procedure uses the Intel 82576 based NIC as an example

1. Browse to the VMware web site, www.vmware.com
2. Select **Support & Downloads**.
3. Select **VMware vSphere**.
4. Select the **Drivers & Tools** tab.
5. Press the **Download** button for the driver for the supported hardware.
6. (In this case VMware ESX/ESXi 4.x Driver CD for Intel 82576 and 82580 Gigabit Ethernet Controller).
7. Press the **Download** button on the details page.
8. Save the iso file to disk.

Prepare the ESX Server

Since the guests in the ESX server need to be shutdown, ensure that this does not interfere with production. Preferably, this should be done during a maintenance stop.

On the ESX server that requires the driver to be applied, logon to each guest node and shutdown the guest in the same manner as if it was a physical computer.

In the vSphere client, select the ESX server, confirm that the guest nodes are shutdown, and place the ESX server into maintenance mode by right-clicking on the ESX server and selecting **Enter maintenance Mode**.

1. Apply the driver using the VMware CLI.
2. Open the iso file using WinZip and identify the offline bundle for the driver.

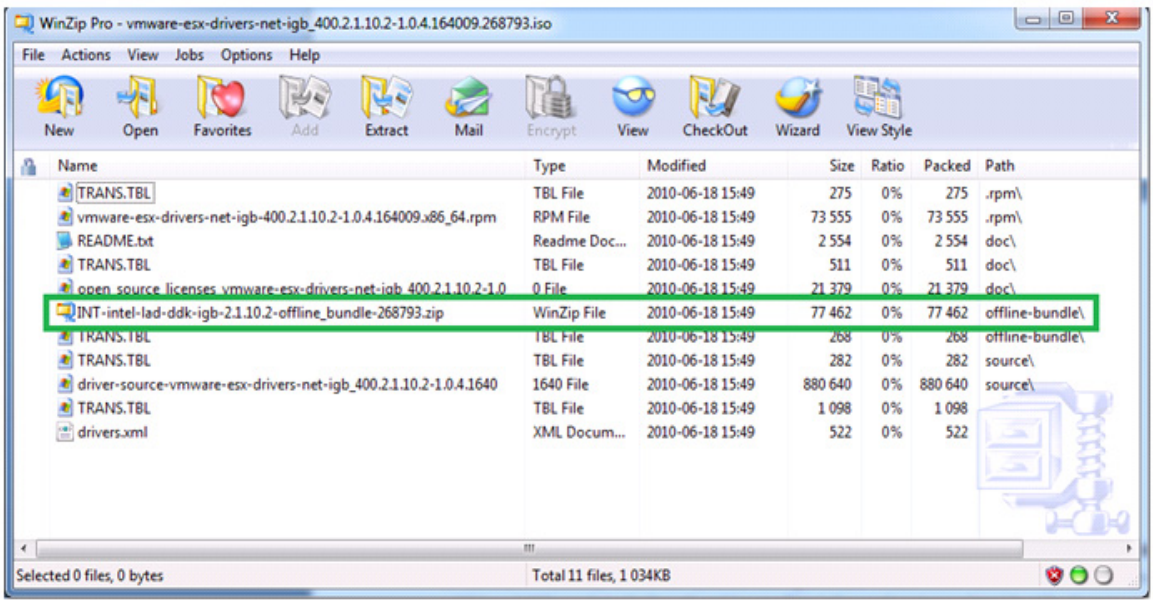
WinZip Pro - vmware-esx-drivers-net-igb_400.2.1.10.2-1.0.4.164009.268793.iso
File Actions View Jobs Options Help
New Open Favorites Add Extract Mail Encrypt View CheckOut Wizard View Style
Name Type Modified Size Ratio Packed Path
TRANS.TBL TBL File 2010-06-18 15:49 275 0% 275 .rpm\
vmware-esx-drivers-net-igb-400.2.1.10.2-1.0.4.164009.x86_64.rpm RPM File 2010-06-18 15:49 73 555 0% 73 555 .rpm\
README.txt Readme Doc... 2010-06-18 15:49 2 554 0% 2 554 doc\
TRANS.TBL TBL File 2010-06-18 15:49 511 0% 511 doc\
open_source_licenses_vmware-esx-drivers-net-igb_400.2.1.10.2-1.0 0 File 2010-06-18 15:49 21 379 0% 21 379 doc\
INT-intel-lad-ddk-igb-2.1.10.2-offline_bundle-268793.zip WinZip File 2010-06-18 15:49 77 462 0% 77 462 offline-bundle\
TRANS.TBL TBL File 2010-06-18 15:49 268 0% 268 offline-bundle\
TRANS.TBL TBL File 2010-06-18 15:49 282 0% 282 source\
driver-source-vmware-esx-drivers-net-igb_400.2.1.10.2-1.0.4.1640 1640 File 2010-06-18 15:49 880 640 0% 880 640 source\
TRANS.TBL TBL File 2010-06-18 15:49 1 098 0% 1 098
drivers.xml XML Docum... 2010-06-18 15:49 522 0% 522
Selected 0 files, 0 bytes
Total 11 files, 1 034KB

Figure 32. Iso file using WinZip

3. Extract this file to the local hard disk. It is preferable to place the file in a short folder name without quotes or directly on the C:\ drive.
4. Start the VMware CLI by selecting **Start - All Programs - VMware - VMware vSphere CLI - Command Prompt**
5. Change directory to the bin folder:

   cd bin
6. Apply the driver using the following command on one line using your ESX server IP, and password:

vihostupdate.pl --server esxipaddress --username root --password yourpassword --bundle c:\ INT-intel-lad-ddk-igb-2.1.10.2-offline_bundle-268793.zip --install

Restart System and Start Guests

1. Restart the ESX server by right-clicking on the ESX server in the vSphere client, and selecting **Reboot**.
2. When the ESX server has restarted, logon using the vSphere client, and confirm that the hardware is now present. For example with the Intel 82576 NIC, select the configuration tab.
3. Exit maintenance mode by right-clicking on the ESX server in the vSphere client, and selecting **Exit Maintenance Mode**.
4. Start each of the guest nodes that were previously running.

Section 10 Upgrading ESX 4.0 Update 1 to ESX 4.1

VMware CLI is a requirement for installing updates.

ESX 4.1 is supported from SV5.1 revision. Performing upgrades of the virtual environment is best performed during a maintenance shutdown to minimize impact on production environments. Before performing any major actions on a computer system, backups should be made. For an 800xA system running virtualized, this means making a backup of the virtual machines, and reviewing the documentation describing the configuration or the ESX server.

When performing the upgrade, the ESX server must be placed in maintenance mode. This means that all of the virtual machines must be either migrated to another ESX server, or be shutdown.

The upgrade is performed from one of the clients connected to the ESX server using the VMware CLI (Command Line Interface)

Download Upgrade Files

1. Browse to the VMware web site, www.vmware.com.
2. Select **Support & Downloads**.
3. Select **VMware vSphere**.
4. Select the **Product Downloads** tab.
5. Scroll down to the Standard product group.
6. Press the **Download** button for VMware ESX 4.1.

7. Logon using your VMware account.
8. In the Download web page, download the zip files for the following items:

   Pre-upgrade package for ESX 4.0 to ESX 4.1

   (File name: pre-upgrade-from-ESX4.0-to-4.1.0-0.0-260247-release.zip)

   ESX 4.1 (upgrade ZIP from ESX 4.0)

   (File name: upgrade-from-ESX4.0-to-4.1.0-0.0-260247-release.zip)
9. Copy the upgrade files to local disk C:\

Prepare ESX Server

Since the guests in the ESX server need to be shutdown, ensure that this does not interfere with production. Preferably, this should be done during a maintenance stop.

On the ESX server that requires the updates to be applied, logon to each guest node and shutdown the guest in the same manner as if it was a physical computer.

In the vSphere client, select the ESX server, confirm that the guest nodes are shutdown, and place the ESX server into maintenance mode by right-clicking on the ESX server and selecting **Enter maintenance Mode**.

Apply Upgrades

1. Start the VMware CLI using by selecting **Start - All Programs - VMware - VMware vSphere CLI - Command Prompt**
2. Change directory to the bin folder typing:

   cd bin

Only install the pre-upgrade-from-ESX4.0-to-4.1.0-0.0-260247-release.zip once. If second attempt to install is made, the subsequent upgrade-from-ESX4.0-to-4.1.0-0.0-260247-release.zip will fail.

3. At the command prompt, enter the following commands below. Each command should be typed as one line. Wait for each to complete before executing the next.

vihostupdate.pl --server esxserverip --username root --password yourpassword -bundle c:\pre-upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip --install

vihostupdate.pl --server esxserverip --username root --password yourpassword --bundle c:\upgrade-from-ESX4.0-to-4.1.0-0.0.260247-release.zip --install

Restart System and Start Guests

1. Restart the ESX server by right-clicking on the ESX server in the vSphere client, and select **Reboot**.
2. Exit maintenance mode by right-clicking on the ESX server in the vSphere client, and selecting **Exit Maintenance Mode**.
3. Start each of the guest nodes that were previously running.

Install the vSphere Client 4.1

1. Browse to the VMware web site, www.vmware.com.
2. Select **Support & Downloads**.
3. Select **VMware vSphere**.
4. Select the **Product Downloads** tab.
5. Scroll down to the Standard product group.
6. Press the **Download** button for VMware ESX 4.1.
7. Logon using your VMware account.
8. In the Download web page, download the exe file for the following items:
   – VMware vSphere Client
9. Install using the default settings.

Upgrade VMware Tools in the Guests

Upgrading VMware tools will require the guest to be restarted.

1. After the guests are started, start the VMware Tools upgrade by right-clicking on virtual machine in the vSphere Client.
2. Select **Guest - Install/Upgrade VMware Tools**.
3. At the Install/Upgrade Tools dialog box, select **Interactive Tools Upgrade** and press the **OK** button.
4. Open a vSphere Client console to the guest node.
5. In the guest node, start the Windows Explorer, select the **DVD drive** and run setup.exe
6. At the Welcome screen, select **Next.**
7. Select **Finish** at the end of the installation.
8. If ok to proceed, accept to restart the virtual machine by pressing Yes in the VMware Tools dialog box.

Changes from ESX 4.0 Update1 to ESX 4.1

USB Memory Sticks

vSphere provides the ability to have USB devices available to the virtual machine guests.

This has the effect that the USB device is no longer available to the COS. In pre-ESX 4.1, this may have been used for transferring files to the ESX server.

To perform the same functionality, use the vSphere client to upload the files to a datastore. In the ESX console, the datastores are located under /vmfs/volumes.

Section 11 Supported 800xA Server Node Types

This section describes the supported 800xA Server Node types.

Support Components

Node Type	Supported
Domain Controller	Yes
Terminal Server	Yes
License Server	Yes
Aspect Server	Yes
Multisystem Integration	Yes
PNSM	Yes

Application Servers

Node Type	Supported
Asset Optimization Server	Yes
Batch	Yes
IM	Yes

Connectivity Servers

Node Type	Notes	Virtualized
AC800M		Yes
PLC Connect		Yes
Foundation Fieldbus		Yes
PROFIBUS/HART		Yes
Advant Master	Use PU410	Yes
MOD 300	Use PU412	Yes
Melody Connect		Yes
Harmony	Use IET800	Yes
IEC61850		Yes
Safety		Yes
DCI Connect		Yes
Freelance		Yes
AC100	Server not virtualized	No

Parts List

Redundant 4 Node 800xA System

For a redundant system with 4 nodes, two ESX servers is required. The following tables outline an example parts list. Note that system configurations may require more resources. For example larger or more hard disks. Refer to *Third Party HW products verified for IndustrialIT System 800xA (3BSE046579*)* for supported hardware. There is also an optional set of components. See Table 6.

Table 2. Primary ESX Server Parts List

Part Type	Description	Quantity	
License	License for Industrial IT, 800xA Software containing the selected 800xA system options.	Per 800xA System	1
	VMware vSphere ESX 4.1 Standard.	Per CPU	1
	Windows 2008 (1)	Enterprise	1
Software	VMware vSphere ESX(i) (3)	Installation Media	1
	Windows 2008	Installation Media	1
	Industrial IT, 800xA Software, installation media.	Installation Media	1
Hardware	HP DL380G7	CPU	1 x 4 Core
		RAM	24 GB
		Hard Disk	8 x 146GB
		Network Adapters	800xA System Dependent
	Rainbow Sentinel SuperPro	USB Dongle (2)	1

Table 3. Secondary ESX Server Parts List

Part Type	Description	Quantity	
License	VMware vSphere ESX(i) (3)	Per CPU	1
	Windows 2008 (1)	Enterprise	1
Hardware	HP DL380G7	CPU	1 x 4 Core
		RAM	24 GB
		Hard Disk	8 x 146GB
		Network Adapters	800xA System Dependent

(1) Refer to the System 800xA, System Guide - Technical Data and Configuration (3BSE041434*) and the Third Party Software System 800xA (3BUA000500) instructions for more information.

(2) This is purchased directly from ABB. The article number is 3BSE034585R1 and is available from the 800xA price book.

(3) Refer to System 800xA 5.1, 5.0, 4.1, 3.1 Third Party Software (3BUA000500) and Security Updates Validation Status for System 800xA (3BSE041902) for specific versions of ESX(i) and supported patch levels. Note that the installation of ESXi is not required as it is ordered with the server, many vendors have ESXi pre-installed on a SD memory card in the server.

Redundant 8 Node 800xA System

For a redundant system with 8 nodes, two ESX servers is required. The following tables outline an example parts list. Note that system configurations may require more resources. For example larger or more hard disks. There is also an optional set of components. See Table 6.

Table 4. Primary ESX Server Parts List

Part Type	Description	Quantity	
License	License for Industrial IT, 800xA Software containing the selected 800xA system options.	Per 800xA System	1
	VMware vSphere ESX(i) (3)	Per CPU	2
	Windows 2008 (1)	Enterprise	2
Software	VMware vSphere ESX 4.1	Installation Media	1
	Windows 2008	Installation Media	1
	Industrial IT, 800xA Software, installation media.	Installation Media	1
Hardware	HP DL380G7	CPU	2 x 4 Core
		RAM	48 GB
		Hard Disk Tray	1
		Hard Disk	16 x 146GB
		Network Adapters	800xA System Dependent
	Rainbow Sentinel SuperPro	USB Dongle (2)	1

Table 5. Secondary ESX Server Parts List

Part Type	Description	Quantity	
License	VMware vSphere ESX(i) (3)	Per CPU	2
	Windows 2008 (1)	Enterprise	2
Hardware	HP DL380G7	CPU	2 x 4 Core
		RAM	48 GB
		Hard Disk	16 x 146GB
		Network Adapters	800xA System Dependent

(1) Refer to the System 800xA System Guide Technical Data and Configuration (3BSE041434*) and the System 800xA 5.1, 5.0, 4.1, 3.1 Third Party Software (3BUA000500) instructions for more information.

(2) This is purchased directly from ABB. The article number is 3BSE034585R1 and is available from the 800xA price book.

(3) Refer to System 800xA 5.1, 5.0, 4.1, 3.1 Third Party Software (3BUA000500) and Security Updates Validation Status for System 800xA (3BSE041902) for specific versions of ESX(i) and supported patch levels. Note that the installation of ESXi is not required as it is ordered with the server, many vendors have ESXi pre-installed on a SD memory card in the server.

Additional External Parts

With the introduction of VMware vSphere 4.1, the ABB licensing dongle can now be used in the guest directly. This makes the use of the AnywhereUSB device optional. There may be instances where it is considered an advantage to have the USB dongle available via the network. Typically, it the virtual machine which runs the licensing server is moved, the dongle does not need to be moved.

Table 6. Optional Devices

Part Type	Description	Quantity	
Hardware	AnywhereUSB from Digi.	Per System	1
	MasterBus Connectivity	PU410	800xA System Dependent
	MOD 300 Connectivity	PU412	800xA System Dependent

Section 12 Storage Area Network

Virtual machines can either be stored on hard disks local in the ESX(i) server, or on a network storage device such as a Storage Area Network (SAN) server. In both cases, the storage is added to the ESX(i) server and seen as datastores.

One advantage of having the virtual machines stored on a SAN server is that the virtual machines can be moved from one ESX(i) server to another. Since both ESX(i) servers have access to the same shared storage, it is only the execution context that needs to be moved rather than the much larger virtual machine hard disk.

This guide provides an overview of SAN and how it is used with VMware vSphere. While SAN servers support either Fiber Channel, iSCSI, or both, this guide only provides information on iSCSI. Most major server vendors also supply SAN servers. The specific configuration of each SAN type is not documented here. Refer to the vendors specific guides for individual device configuration details.

It is essential that the configuration used is confirmed to function as expected before used for production. This includes using the performance monitors in the ESX(i) servers to ensure that load balancing is operational and to ensure that network redundancy is working by temporarily removing network connections.

SAN Hardware

SAN servers are highly redundant disk arrays that provide storage over a network. Each SAN has redundant power supplies, redundant controller modules, redundant network connections per controller module and redundant disks.

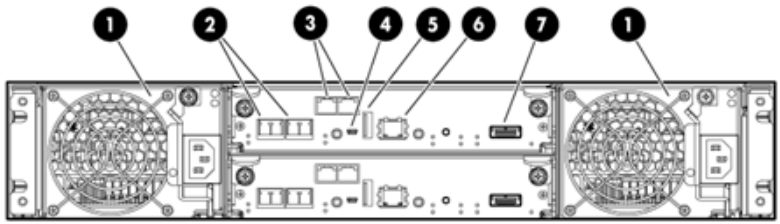

Figure 33. Rear View of an SAN Device

The following parts as numbered in the Figure 33 are:

1. Power Supplies.
2. Fiber Channel host ports.
3. iSCSI ports (host or replication).
4. CLI port (mini-USB).
5. Reserved for future use.
6. Management Ethernet port.
7. SAS expansion port.

SAN Storage Configuration

SAN servers typically consists of 12-24 hard disks. These are normally configured as one or more RAID 5 (block-level striping with distributed parity) disk groups with a number of disks set as **hot spares** or **hot standby** used as a failover mechanism to provide reliability in System Configurations. The SAN server vendor may have best practices for allocation of the storage.

When combining disks to create RAID arrays, a storage item is created which is used to create virtual disks. These are the entities that become available as datastores in ESX(i).

Always remember that the largest size for a datastore is 2TB - 512Bytes.

When formatting datastores, the file block size may need to be changed to accommodate the largest file that is created in the datastore.

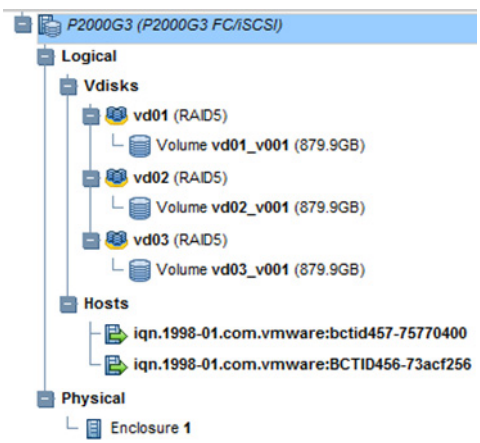

Figure 34. SAN Server Storage Configuration

SAN Networking

Figure 35 and Figure 36 provides an overview of the networking required for a SAN server implantation.

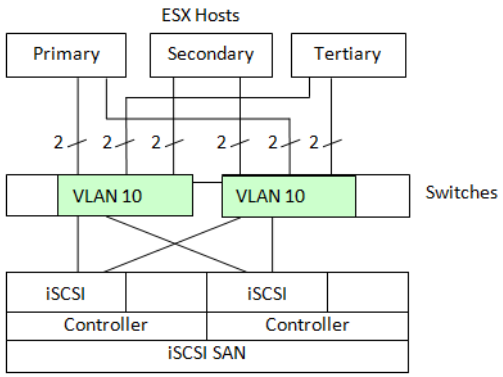

Figure 35. SAN Storage iSCSI Network

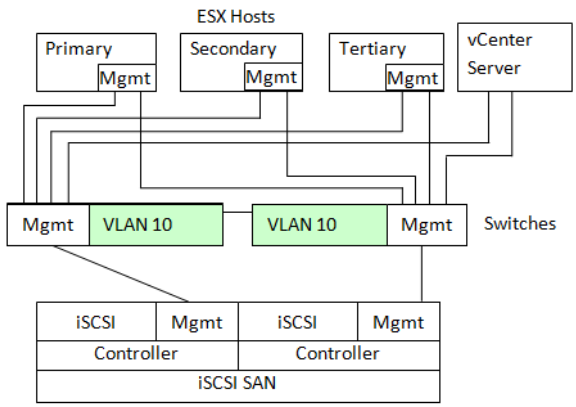

Figure 36. SAN Storage Management Network

One or more ESX(i) servers are connected to multiple network switches through multiple network connections. The SAN server is also connected to the switches through multiple network connections.

There are two types of network traffic in this configuration. One is for access to the shared storage through iSCSI. The other is for configuration and management of the servers. To provide security and reliability, the two types of traffic are separated using a VLAN.

To reduce single point of failures, separate network adapters should be used in the ESX(i) servers for the storage network as shown in the Figure 37.

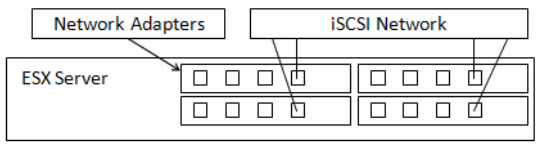

Figure 37. Multiple Network Adapter Connection for Higher Reliability

While the multiple network connections provide redundancy, it also provides load balancing. Figure 38 provides an example of IP addresses for the storage network.

When configuring the IP addresses in the SAN server, the VLAN settings may be in the advanced settings as shown in the Figure 39.

In the Figure 40, it is observed that the SAN server does not support VLAN. In this case, separate network switches for iSCSI and management traffic should be used.

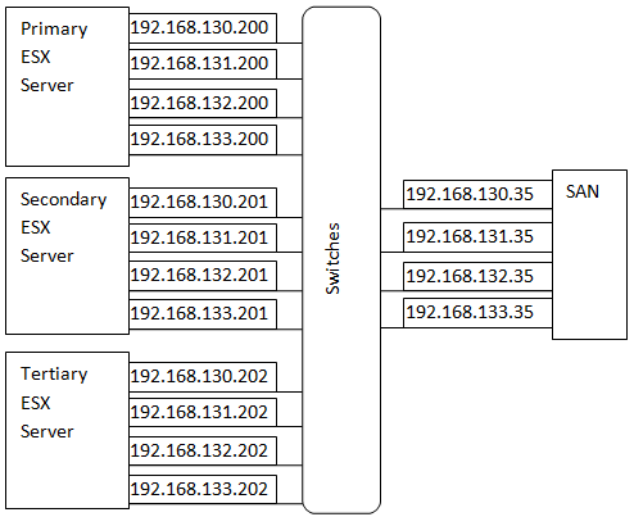

Figure 38. IP Address for the Storage Network

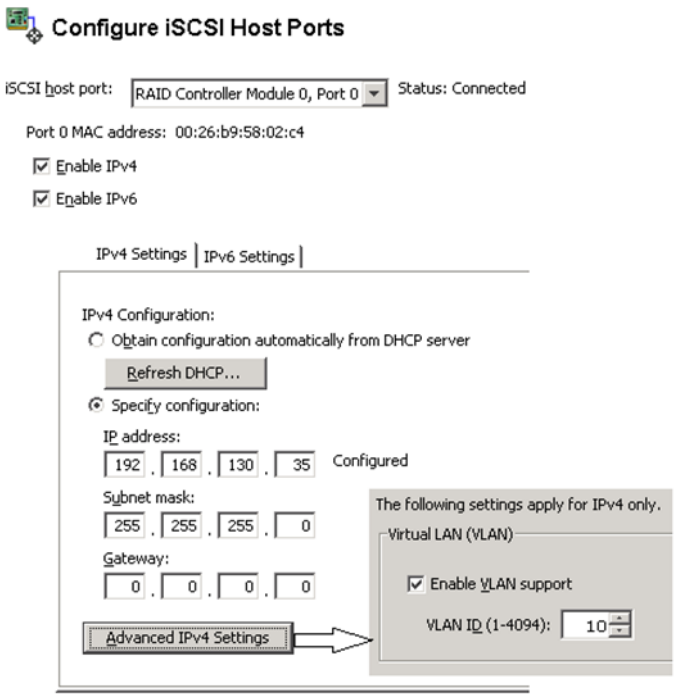

Figure 39. Setting the VLAN ID for the iSCSI Ports

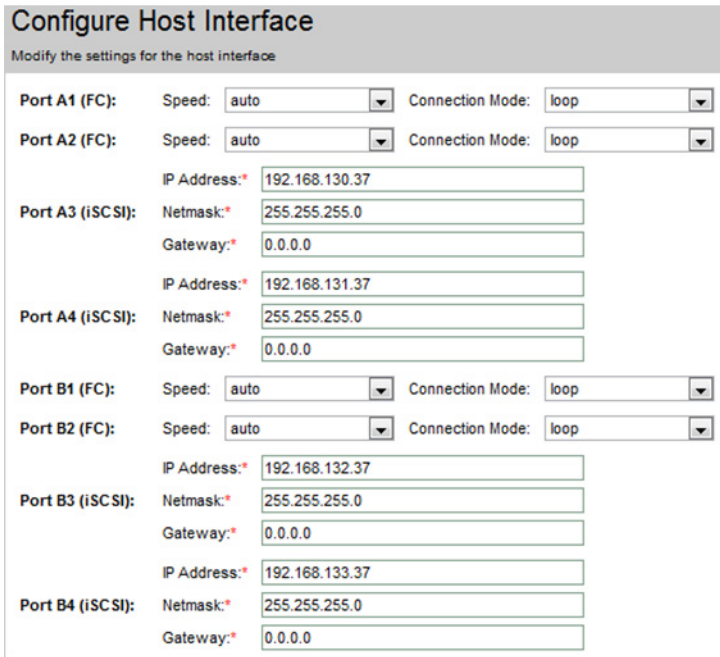

Figure 40. SAN Server iSCSI IP Configuration

ESX Server Network Configuration

Implementation of networking for the virtual solution involves separating functionality and implementing redundancy. There should be separate networks for the management and SAN iSCSI storage networks. This prevents management network traffic from interfering with the storage network traffic. Figure 41 shows the network configuration. Hardware vendor guidelines may recommend different configurations but, the configuration should always be verified that network utilization is optimized.

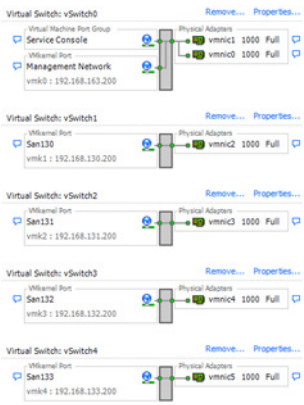

Figure 41. ESX Server Network Configuration

Adding in Datastores

This description is based on using the iSCSI Software Adapter in the ESX Server.

Perform the following steps in the ESX Server:

1. Select the **Configuration > Storage Adapters Configuration**.
2. Select **iSCSI Software Adapter**.
3. On the **Details**, select **Properties...**.
4. In the `iSCSI Initiator Properties`, select **Configure...**.
5. Select **Enabled** and click **OK**.

6. On the **Dynamic Discovery** Tab, for each SAN IP Addresses, perform the following steps.
   - Select **Add...**. Enter the IP Address of the iSCSI Server and click **OK**.
   - Click **Close** once all the IP Addresses are added.
   - A message appears to `Rescan the Host Bus Adapter`, click **Yes** to rescan.

If the iSCSI storage server is not used before, the datastores must be added and formatted. The procedure is same as adding a local storage disk.

When formatting the datastores it is important to consider the largest file size and set an appropriate block size.

If the iSCSI storage server is already been used in an ESX server, then the datastores appears in the storage configuration without the intervention of the user.

Load Balancing

Perform the following steps to manage the paths:

1. Select the **iSCSI Software Adapter**.
2. On the **Details**, the devices list appears as shown in the Figure 42.

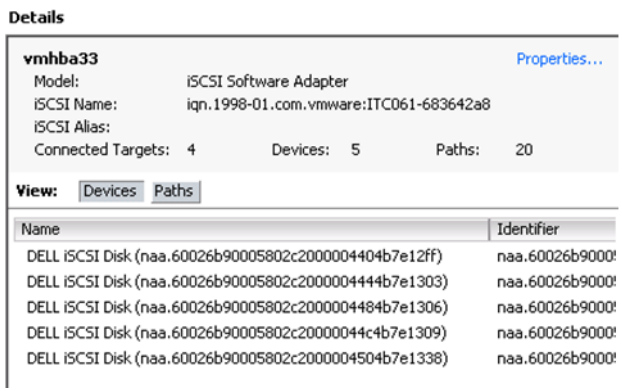

Figure 42. iSCSI Device Details

3. Choose a device, right-click and select **Manage Paths...**.

4. On the Manage Paths window, select **Round Robin** from the `Path Selection` (Figure 43).

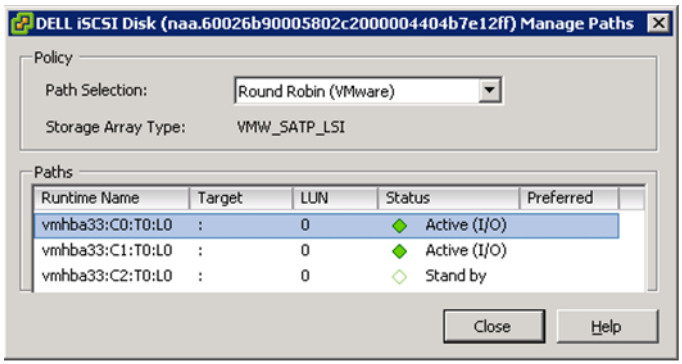

Figure 43. iSCSI Path Selection Policy

Performance

It is essential that the configuration provides the best performance before using in a production environment. This involves monitoring the throughput to the datastores and ensuring that all networks are being used.

In the network performance chart below, the 4 network adapters that are supporting the SAN server 1,3,4,7 (Figure 44) are all providing throughput to the SAN sever.

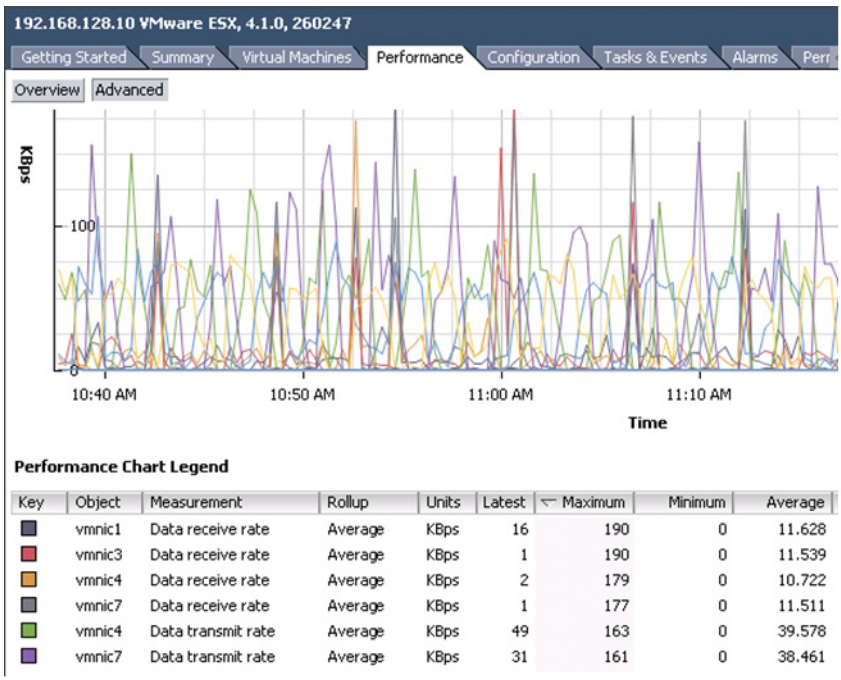

Figure 44. Load balancing of SAN Servers

If the configuration is not correctly setup, not all the network connections used for communication with the SAN server. It displays the network traffic. It is important to check the average/maximum values as there may be instances where the network traffic was sampled when there was no traffic.

The following are the areas that must be checked:

- Are the network switches in the ESX(i) server configured correctly.
- Are the VLANs setup correctly in the ESX(i) server and the SAN server.
- Can the SAN server be pinged on each of the IP addresses from the ESX(i) server. Note that vmkping is used from the console of the ESX(i) server.
- Is it iSCSI Path Selection Policy set to Round Robin.

- Does the SAN server has a preferred path that needs to be reset or reconfigured.
- Contact the SAN supplier for additional information regarding configuration.

Section 13 VMware vCenter Server

When ESX(i) servers in a computing environment increases, the time and effort to maintain the individual servers also increases. Consider changes in user access would need to be applied to each ESX(i) server individually. To make this job easier, VMware developed the vCenter Server.

Additional capabilities are also unlocked once the ESX(i) servers have been added to the vCenter server. These include VMware High Availability, vMotion, Storage vMotion, and Fault Tolerance. Inclusion of the capability depends on the license applied to the ESX(i) server.

To facilitate these advanced functionalities, the virtual machines need to be stored on a Storage Area Network (SAN) device. This is a highly redundant disk storage unit which uses either Fiber Channel, or Internet SCSI (iSCSI) to communicate to the ESX(i) servers. The folder that represents the virtual machine (including the virtual hard disk, and configuration files) is stored in the SAN device. Typically, the SAN device has RAIDed storage, redundant controller cards, redundant power supplies and multiple network connections per controller card (Figure 45).

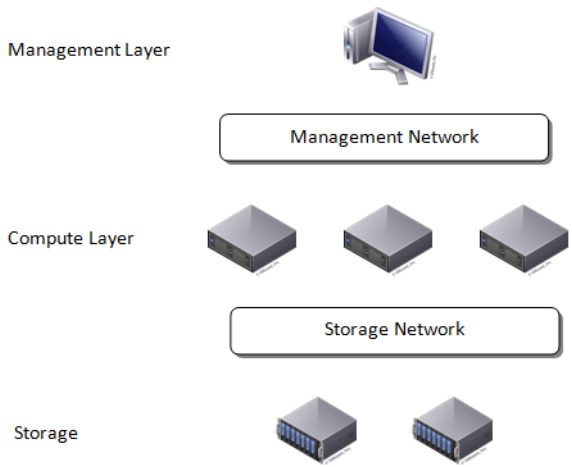

Figure 45. Enterprise Virtualization Components

vCenter Server is not included in VMware vSphere ESX(i) and must be purchased separately to implement VMware vSphere advanced functionality such as VMware High Availability.

It is important to remember that the free version of ESXi cannot be added to a vCenter Server. A full license for the features required must be purchased and used to replace the free license.

vCenter Server is a product that runs on Windows 2008 Server (64-bit) and should be installed into a computer dedicated to run the vCenter Server. Hence, vCenter Server should not be installed on a domain controller, 800xA Server or 800xA Client Node. vCenter Server stores information into a Microsoft SQL Server database. For installations of small number of ESX(i) servers, it is better to install Microsoft SQL Server Express that is included in the vCenter Server installation media.

While it is not a pre-requisite to have external storage for vCenter Server, advanced functionality such as VMware High Availability requires virtual machines stored in an external storage unit accessible over the network.

The same VMware vSphere Client that is used to interact with the individual ESX(i) servers is also used to interact with the vCenter Server. When logging into the

vCenter Server, Windows accounts for the computer where vCenter Server is running.

User Accounts

When ESX(i) hosts are added to a vCenter server, the user accounts that pertain to the computer running the vCenter server can be used to set permissions for the ESX(i) hosts. It is therefore, important to plan if the vCenter server is to be a member of a domain, or a standalone server.

Installation Procedure

Ensure to install the MS SQL Server Express Edition that comes with the vCenter installation media before performing the Installation procedure.

Pre-requisites

Windows 2008 Server 64 bit:

- Do not combine with a Domain Controller.
- Preferably a computer dedicated to running vCenter Server.
- Can be a virtual machine. All possible hardware failures and effects caused by the loss of vCenter Server must be accounted for.

Installing vCenter Server

Perform the following steps to install the vCenter Server:

1. Insert the vCenter installation media to install the vCenter.
2. On the **VMware vCenter Installer**, select the **vCenter Server** from the `VMware Product Installers list`.
3. On the **Choose Setup Language**, select the language and click **OK**.
4. On the **Welcome** window and click **Next**.
5. On the **End-User Patent Agreement** and click **Next**.
6. Read and Accept the terms in the license agreement and click **Next**.
7. Enter User Name, Organization, and License key details. Click **Next**.

The User Name is not a login account.

8. Leave the *Install a Microsoft SQL Server 2005 Express instance* on the **Database Options** window and click **Next**.
9. Leave the *Use SYSTEM Account* and click **Next**.

   If the User-Specified account is used, the following conditions must be satisfied:

- The user-specified account must be an Administrator on the local machine, who acts as a part of the operating system, and logins with service rights.
- User must specify the account name as DomainName\Username in the vCenter Server install wizard.
- Configure the SQL Server database to allow the domain account access to SQL Server.

10. On the **Destination Folder** window, click **Next**.
11. Leave the *Create a standalone VMware vCenter Server instance* on the **vCenter Server Linked Mode Options** window and click **Next**.
12. Leave the ports at default on the **Configure Ports** window and click **Next**.
13. Select the **Inventory Size** to Small (less than 100 hosts) on the **vCenter Server JVM Memory** window and click **Next**.
14. Click **Install** on the **Ready** window to install the program.
15. Click **Finish** on the **Installation Completed** window.

Installing vSphere Client

Perform the following steps to install the vSphere Client:

1. Select **vSphere Client** from the `VMware Product Installers list`.
2. Select the **Setup Language** and click **OK**.
3. On the **Welcome** window and click **Next**.
4. On the **End-User Patent Agreement** and click **Next**.
5. Read and Accept the terms in the license agreement and click **Next**.
6. Enter User Name, and Organization. Click **Next**.
7. On the **Destination Folder** window, click **Next**.
8. Click **Install** on the **Ready** window to Install the Program.
9. Click **Finish** on the **Installation Completed** window.

Configuring vCenter Server

Logging into the vCenter Server is performed either locally or remotely. When logging in locally on the vCenter Server, the IP address is set to localhost, and `Use Windows session credentials` is selected.

The Getting Started tab provides an overview to the first step in configuring the vCenter Server.

Adding a Datacenter Object

Before adding ESX(i) servers to the vCenter Server, a datacenter object must be created:

1. Right-click on the **vCenter Server** icon on the left pane and select **New Datacenter.**
2. Enter a name for the datacenter.

Adding an ESX(i) Server

ESX hosts are added to datacenter objects, or cluster objects. If an ESX(i) server is moved between objects, then there may be a requirement of not having to run the virtual machines on the ESX host.

Perform the following steps to add an ESX(i) Server:

1. To add an ESX host to the vCenter Server, right-click on either a `datacenter object` or a `cluster object` and select **Add Host**.
2. Enter the IP address of the host or the name of the host if DNS is available.
3. Enter the username and password of the ESX(i) host. Normally, the username is the root.
4. Click **Yes** on the **Security Alert** window to trust the host.
5. On the **Host Summary** window click **Next**.
6. Enter the license for the ESX(i) host in the **Assign License** window. Click **Next**.

This cannot be the free ESXi host license.

7. Leave the **Enable Lockdown Mode** unchecked on the **Lockdown Mode** window and click **Next**.
8. Select the location for the ESX host on the **Virtual Machine Location** window and click **Next**.
9. Review the summary and click **Finish** on the **Ready to Complete** window.

Limitations when Interacting with ESX(i) Servers

After ESX(i) hosts are added to the vCenter Server, a number of options are enabled. They are not described in this guide. The following is a limitation when interacting directly with the ESX server, or through vCenter Server:

- When opening a console to a virtual machine through the vCenter Server, the option to `Fit Guest Now` may be disabled. The workaround to this problem is to log directly into the ESX(i) server and then open a console. It may be required to restart the VMware Tools Service in the virtual machine.

Section 14 Improving Availability

This section describes how to improve the VMware high availability.

VMware High Availability is not a substitute for 800xA redundancy.

The VMware High Availability (HA) functionality is designed to recover ESX(i) servers automatically from a hardware failure. Virtual machines that are running on the failed server are automatically restarted on another ESX(i) server. There will be some minutes from the detection that the virtual machines are offline to the restarted virtual machines restoring services. The configuration of VMware HA allows the specification of the ESX server that hosts the restarted virtual machines.

VMware HA requires that the virtual machines are stored on an external storage server such as a SAN server, and that the ESX(i) Servers are added to a vCenter Server. The storage network and the management network must be redundant.

With the introduction of USB support in ESX(i) 4.1 it is possible to have the ABB USB dongle connected directly into the ESX(i) server and available in the guest. However, when a virtual machine is moved from one ESX(i) server to another it is necessary to move the dongle as well. Here, it would be beneficial to use a USB over IP device such as AnywhereUSB to maintain continuity of functionality when moving virtual machines.

Configuring VMware High Availability

Before configuring VMware HA, the network setup should be reviewed. Refer to section ESX(i) Server Configuration.

When a virtual machine is moved from one ESX(i) server to another, the vSwitches must have the same set of names. For example, if the plant network is named PN1 on ESX1, then it must also be named PN1 on ESX2 and ESX3.

The ESX(i) servers that are part of the VMware HA configuration must also be part of a cluster in the vCenter Server as shown in the Figure 46.

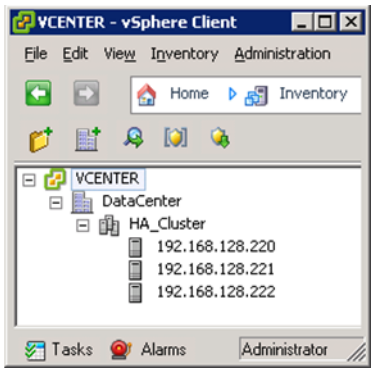

Figure 46. Cluster in vCenter

Adding a Cluster Object

Perform the following steps to add the cluster:

1. Log in to the vCenter Server.
2. If there is no DataCenter, create one by right-clicking on the **vCenter object** in the left pane, selecting **New DataCenter** and providing a name for the datacenter.
3. Right-click on the **DataCenter** object, and select **New Cluster…** to create a cluster.
4. Enter a name for the cluster, select the **Turn On VMware HA** option and click **Next**.
5. Leave the Host Monitoring Status and Admission Control properties in their default settings. These can be adjusted later. Click **Next**.
6. Leave the Cluster Default Settings as their default settings and click **Next**.
7. Leave the VM Monitoring Status and Default Cluster Settings as default and click **Next**.

8. Leave the Enhanced vMotion Compatibility (EVC) disabled.
9. Leave the Swapfile Policy for Virtual Machines as default and click **Next**.
10. Review the summary of settings and click **Finish**.

Adding ESX(i) Servers to the Cluster

To add ESX(i) servers to the cluster, the following procedure is repeated for each ESX server:

1. Right-click on the cluster object and select **Add Host…**
2. Enter the Host name or IP address, Username, and Password and click **Next**.

If the name is used, the vCenter and ESX hosts must have a functioning DNS server.

3. Click **Yes** on the **Security Alert** window.
4. Click **Next** on the **Host Summary** window.
5. Enter the license for ESX(i) server if it is not entered previously and click **Next**.

This cannot be the free ESXi host license.

6. Leave the **Enable Lockdown Mode** unchecked on the **Lockdown Mode** window and click **Next**.
7. Click **Finish** on the **Ready to Complete** window.

Specifying Failover Host

In the SAN Networking on page 112, the three ESX(i) servers in the configuration. The primary server is used for the primary 800xA nodes, while the secondary server is used for the redundant 800xA nodes. The third server in the configuration is the failover host (Figure 47) that is not running virtual machines. If either the primary or secondary server fails, the virtual machines that were running on the failed server is started on the third server.

To ensure that the failed nodes on the primary server are not started on the secondary, or visa-versa, it is important to specify the third server as the failover server:

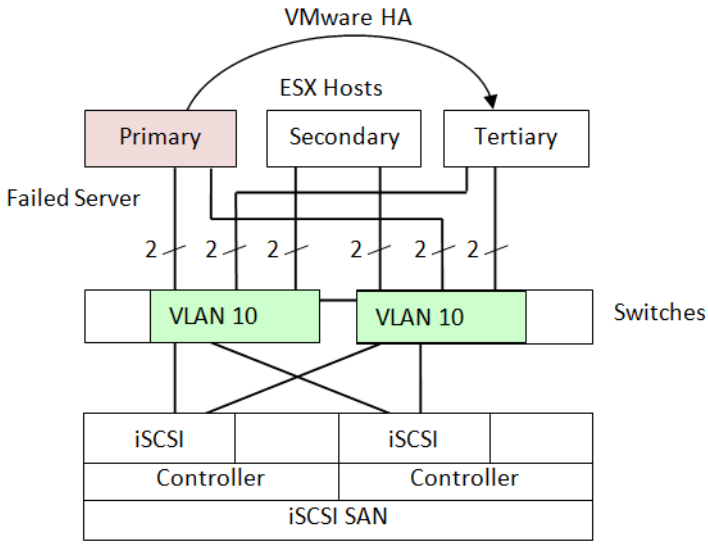

Figure 47. VMware High Availability Restarts the virtual machines on the failover server

1. Right-click on the Cluster object and select **Edit Settings…**
2. Select **VMware HA** on the left pane.
3. Enable `Do not power on VMs that violate availability constraints` on the Admission Control in the right pane.
4. Select `Specify a failover host` and select the third ESX(i) server from the drop-down box on the Admission Control Policy.
5. Click **OK** to complete.

VMware vMotion

VMware vMotion must not be used during production, only for maintenance operations during a maintenance stop of the factory.

VMware vMotion is the ability to move virtual machines from one ESX(i) server to another while it is running. It is required that the ESX(i) servers are members of a vCenter server and that the virtual machines are stored on a SAN server.

When a vMotion operation is performed, the memory of the virtual machine is progressively transferred to the other ESX(i) server. Changes in the memory of the original virtual machine are tracked and transferred. When the remaining memory to be transferred is small enough to be performed in one last operation, the virtual machine is stopped, the remaining memory transferred, and the virtual machine execution is continued on the other server. This generally results in a loss of one ping on the network. Depending on the network speed and the CPU activity of the virtual machine, this time may be more or less.

It is important to keep in mind that while the loss of network connection may be in the order of a few seconds, applications and services on the computer transferred, or communicating with the computer transferred may take longer to return to normal operations.

To assist in minimizing interference with the storage network communication, a separate network should be used for vMotion operations.

VMware Storage vMotion

VMware Storage vMotion is not supported for System 800xA.

VMware Fault Tolerance

VMware Fault Tolerance is not supported for System 800xA.

Section 15 800xA in the IT Infrastructure

Many companies have an IT infrastructure and have already taken advantage of virtualization for consolidating server functionality. Moving the 800xA Server environment to the IT infrastructure is a logical progression for optimizing both hardware and IT expertise.

While there is a diverse hardware range in the IT infrastructure, only VMware vSphere ESX(i) servers that are running on Intel servers are supported for 800xA.

Typically, these types of environments make heavy usage of SAN storage.

Generally, monitoring of the server hardware is already in place but not integrated into 800xA in these installations. The procedure to notify production environments of server issues needs to be reviewed.

While the 800xA Server nodes can share resources with other servers, it should be considered as a best practice to have the 800xA Server nodes residing on ESX(i) servers and storage units that are not being shared with other servers. If there is some sharing, the resource usage should be reviewed. This includes the typical loading of scheduled or unscheduled activities such as weekend backup operations. The 800xA is a 24/7 system and should have resources accordingly.

Those who are responsible for maintaining the infrastructure must be aware that the 800xA System is a 24/7 System which cannot be treated in the same fashion as other servers. Maintenance must always be coordinated with production to ensure that no downtime occurs.

Due to the diversity of configurations, ABB cannot fully support the various configurations possible. The project and customer must be in agreement regarding support responsibilities before the project is undertaken. This includes the required knowledge and resources to assume the responsibility of support.

Section 16 Virtual Client

800xA workstations are dedicated physical computer workstations running Windows 7 and 800xA as an operator client. Moving the physical clients to the virtual environment allows the benefits of virtualization to be extended to the clients.

Virtual clients (Figure 48) are virtual machines which are running Windows 7 and 800xA as an operator client. Access to the virtual client desktop is done over the network through a thin client which has 1to 4 monitors, a keyboard and a mouse attached. In the first release of virtual client support for 800xA, only Microsoft remote desktop protocol is supported.

Thin clients are purpose built computers from hardware vendors such as HP and Dell. These devices normally have low power consumption and runs without a fan. The operating system pre-installed in these devices need to be Windows 7 to handle multiple screen remote sessions and is usually installed on an internal flash device.

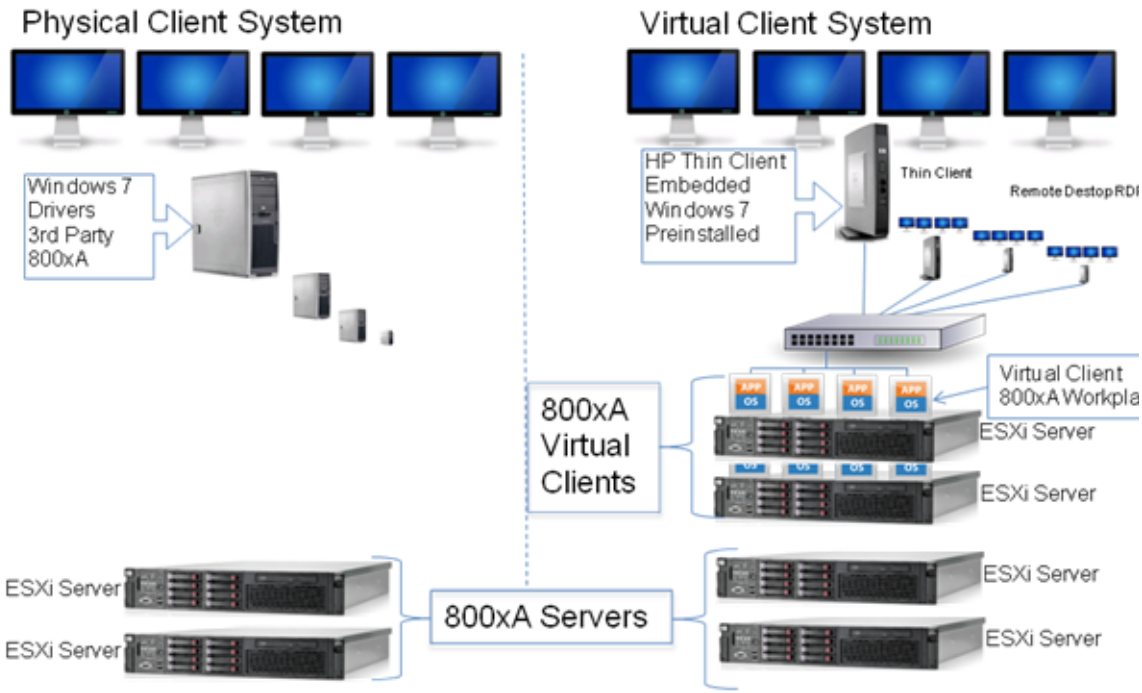

Figure 48. Physical Client to Virtual Client Comparison

Microsoft allows multiple screen remote sessions in the following versions of Windows:

- Windows 7 Enterprise - 32-bit (x86) and 64-bit (x64)
- Windows 7 Ultimate - 32-bit (x86) and 64-bit (x64)
- Windows 2008 Server R2 - 64-bit

Virtual Terminal Server

Virtual terminal servers share many similarities to virtual clients. They are both virtual machines running a Windows operating system and are connected through a thin client over the network. The main difference in the terminal server solution is that multiple users login to the same terminal server which is running Windows Server 2008 R2 instead of Windows 7. For the virtual terminal server, 800xA is installed into a virtual machine using the same method as a physical terminal server. As there are more concurrent users in the virtual terminal servers, the virtual machine where the virtual terminal server resides requires more virtual CPU and RAM allocated.

Figure 49 shows a comparison between a physical terminal server solution and a virtual terminal server solution.

Whilst the diagram shows that the virtual terminal servers are added as additional 800xA virtual nodes in the existing virtual hosts, depending on the number of users and loading in the virtual terminal server, the virtual terminal servers may need to be moved to additional virtual hosts.

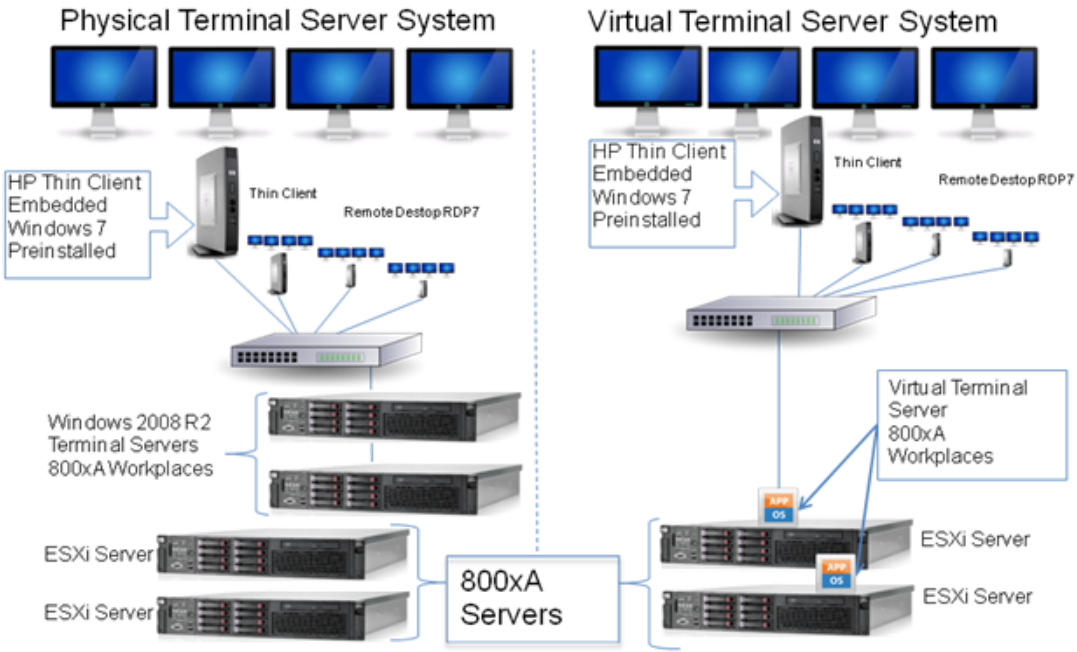

Figure 49. Physical Terminal Server to Virtual Terminal Server Comparison

Benefits of Virtual 800xA Workplaces

The following are the benefits of virtual 800xA workplaces:

- Reduced operator room space requirements
- Reduced operator room power and heating requirements
- Reduced operator room cooling requirements
- Reduced operator room noise
- Fast replacement of thin client
- Ability to move virtual client to new hardware without reinstall
- Standard installation without messing the drivers
- Added security by setting up virtual client without USB
- Clients now in server room with cost effective remote solutions

When considering relatively small number of clients that are involved in an 800xA solution compared to the enterprise client virtualization, the initial cost of a virtual client solution is at a disadvantage. However, the subsequent maintenance benefits are a continuous benefit that should always be considered when engineering solutions.

Comparison of Virtual Client and Virtual Terminal Server

Whilst virtual clients and virtual terminal servers benefit from virtualization, there are some practicalities that need to be considered while deciding which technology to implement.

When considering updating of the systems, there are fewer terminal servers than virtual clients, hence, there is less work to update the system. However, if the terminal server needs to be restarted, more users will be affected.

Virtual clients offer full isolation between users. Only one user can logon to a virtual client where as many users can logon to a terminal server. Hence, with virtual clients, action of one user cannot interfere with other users.

Licensing for Microsoft Office in terminal servers is more complicated than Windows 7 clients and should be investigated before implementing the terminal server solution.

Control Room Planning

When consolidating hardware into virtual systems, availability must always be considered. If a control room has all clients consolidated into one virtual server host and that host becomes unavailable, there will be no clients available. Hence, there must be at least 2 ESXi servers supporting the control room clients.

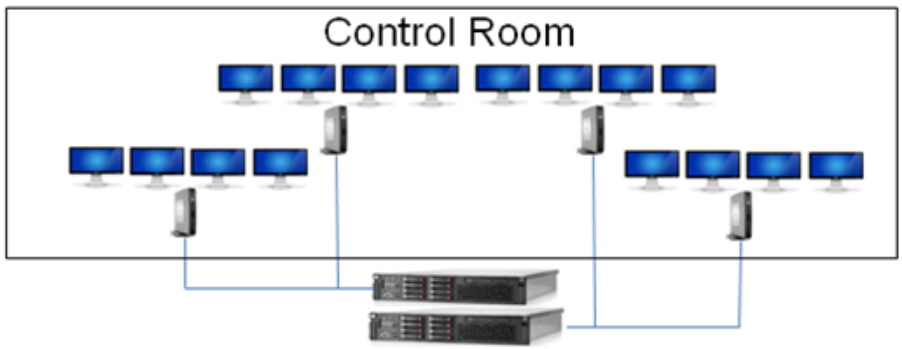

Figure 50. Control Room Support from Multiple Physical Servers

A separate network for the remote access must be configured. This enables secured firewall configurations, which improves security by keeping the remote access separate from plant and control networks.

Graphical Presentation and Physical Server Speed

Graphical rendering that is presented using the thin client is created in the virtual node using virtual, and hence physical, CPU resources. The virtual machine does not take advantage of the physical server graphics adapter capabilities. Specifying the physical server CPU should take this into account. If the 800xA workplaces are expected to be heavily loaded, then a faster CPU would provide more capability to handle the load.

Configuring the Virtual Client Virtual Server Hardware

Since graphic presentation is of high importance in a virtual client solution, it is important to consider this when selecting a server configuration. The virtual central processing unit (CPU) and the physical server CPU cores are responsible for rendering graphics. A faster CPU would have more capacity for rendering graphics than a slower CPU.

A virtual client is defined as a Windows 7 virtual machine. Windows, VMware Tools, Third party software, and 800xA are installed.

Virtual Client

When considering the dimensioning of a virtual client, two virtual CPUs must be allocated to the virtual machine. The 800xA workplace when heavily loaded, may consume one virtual CPU capacity. As there are many other processes in a Windows computer, it is not desired to have their activity interfere with the virtual CPU that is supporting the 800xA workplace. Whilst there is no strict definition that one virtual CPU is allocated to the 800xA workplace and no other task, having an additional virtual CPU provides an available CPU resource for other processes in the virtual computer.

Table 7 provides an example of the virtual machine for a virtual client.

Table 7. Virtual Machine for a Virtual Client Example

Item	Value
OS	Window 7
No of vCPU	2
RAM	4 GB
Video RAM	128 MB
Hard Disk	60 GB

Whilst there may be an idea that adding more virtual CPUs may increase performance, it should be realized that before a virtual machine can be given a slice of physical CPU resources, VMware ESXi must allocate all of the virtual CPUs to physical logical processors at the same time. If the virtual machine has a higher virtual CPU count, and there are more total virtual CPUs running than physical logical processors, there may be a delay in the virtual machine execution. This could result in a performance impact. Hence, increasing the number of virtual CPUs in a virtual machine may not result in a performance improvement.

VMWare ESXi Server Dimensioning for Virtual Clients

When determining the minimum physical server hardware requirements, the sum of the virtual client definitions is summated. This is only the minimum, and the additional resources should always be factored.

For the physical CPU, there should be the same or more physical logical processors as there are virtual CPUs.

A physical CPU hyper-threaded core has two physical logical processors.

Table 8 provides a guide for understanding the minimum requirements of the physical server based on the number of virtual clients.

Table 8. VMware ESXi Server Dimensioning for Virtual Clients Example

Max No of Virtual Clients	Minimum Server Hardware Requirements			
	No of CPUs (with HT)	No of Logical CPUs	RAM	Total Hard Disk
4	1 x QUAD CORE	1x4x2 => 8	24 GB	300 GB
6	1 x SIX CORE	1x6x2 => 12	32 GB	480 GB
8	2 x QUAD CORE	2x4x2 => 16	48 GB	600 GB
12	2 x SIX CORE	2x6x2 => 24	64 GB	960 GB

If there are other virtual machines running in the physical server, their resource requirements are to be added to the virtual client resource requirements.

Configuring the Virtual Terminal Server Virtual Server

When considering configuration of the virtual terminal servers and physical server, there are a number of factors that will provide guidance. These factors revolve around the loading of the virtual terminal servers and capacity of the server hardware.

Loading of the virtual terminal server is a factor of how many concurrent users are logged into the virtual terminal servers, and what type of activity are they

performing. For example, a user that logs on and looks at few of the documents will produce lower loading than a user that logs on from a 4 screen thin client, calls up a 4 screen 800xA workplace and a quantity of alarms and trend displays.

Loading of a computer is typically in the form of CPU, RAM and disk usage. As with most graphical interfaces, the 800xA workplace presentation is supported by one of the threads in the application. When the quantity of display objects is increased, the loading to display the objects is increased. If the loading becomes too high, the thread will reach the full capacity of a single physical logical processor, and the workplace response to user interaction will become slower. This provides a measure of overloading the virtual terminal server session. To minimize the impact on other users, there should be one virtual CPU per terminal server session and one physical logical processor per virtual CPU. As with all computers, there are many other processes in the background which require CPU access. Hence, along with the virtual CPUs that have been specified for the terminal server sessions, at least one additional virtual CPU should be added for background tasks.

If there are more virtual CPUs than physical logical processors, there may be a performance impact depending on the overall loading of the physical server as the virtual machines may have to wait to access physical logical cores.

Considering that the physical CPU is ultimately responsible for rendering graphics, a faster physical CPU provides better capability than a slower one.

When considering RAM, the virtual terminal server operating system needs 2GB of RAM, and each concurrent terminal server session should have 1- 2GB of RAM. For the hard disk, additional hard disk capacity should be added to cater for user local storage requirements.

In some cases, the virtual terminal servers will be in a virtual host with other 800xA nodes. The requirements for all virtual nodes should be summated to establish the total physical requirements for the physical server.

Terminal Server Definition

Considering that there are many varying factors involved in the usage of a terminal server, an initial recommendation should be considered, a guidance which should be updated based on experience. Some installations may have sparsely populated 800xA graphic displays, whilst others are more heavily populated across more monitors. Providing additional capacity in the form of virtual and physical resources

reduces the potential for performance issues. Once the operating conditions have been monitored, the decision to provide more capacity and more users can be considered.

A virtual terminal server is defined as a Windows 2008 R2 virtual machine. Windows, VMware Tools, Third party software, and 800xA are installed.

Table 9 provides an example to the concept of defining the virtual machine that the virtual terminal serve is to run in based on the expected number of concurrent users. Note that, based on the level of loading that the user session creates, it is possible to have more or less users per terminal server. As this is a factor of what the users are doing, and the CPU speed of the physical server, this cannot be accurately determined beforehand. This table provides an example for the dimensioning of a virtual terminal server based on the number of concurrent users.

Table 9. Virtual Terminal Server Virtual Machine Example

No of Users	Virtual Terminal Server Definition			
	vCPU	RAM	Video RAM	Total Hard Disk
1	2	2 GB	128 MB	80 GB
2	3	4 GB	128 MB	90 GB
3	4	6 GB	128 MB	100 GB
4	5	8 GB	128 MB	110 GB
5	6	10 GB	128 MB	120 GB
6	7	12 GB	128 MB	130 GB

When defining the virtual machine, the operating system is set to Windows 2008 R2.

VMWare ESXi Server Dimensioning for Virtual Terminal Servers

There are many factors involved in providing adequate physical computer resources for the virtual environment. The physical server supports other 800xA virtual nodes. When specifying physical hardware, the requirements of all virtual nodes are

summated to have a starting minimum physical resource definition. Expansion through redefining the virtual nodes with more resources, of adding additional virtual nodes should also be added into the minimum definition.

Table 10 shows an example of defining server hardware based on the number of users on virtual terminal servers.

Table 10. VMware ESXi Server Dimensioning Example

No of Concurrent Users	No of Virtual Terminal Servers	Minimum Server Hardware Requirements			
		No of CPUs (with HT)	No of Logical CPUs	RAM	Total Hard Disk
6	1	1 x QUAD CORE	1x4x2 => 8	16 GB	130 GB
8	2	1 x SIX CORE	1x6x2 => 12	24 GB	240 GB
12	2	2 x QUAD CORE	2x4x2 => 16	24 GB	260 GB
16	3	2 x SIX CORE	2x6x2 => 24	64 GB	360 GB

When a larger number of users are involved, it is recommended to have multiple virtual terminal servers. When a virtual node has more virtual CPUs allocated to handle the load, the process of providing physical CPU resources may have a performance impact. To determine level of runtime loading of the virtual terminal server, the task manager in the virtual terminal server is called up, and checked to see if any process is consuming a full logical processor in CPU loading. Note that for example, if a virtual terminal server has 4 virtual CPUs, a process that has 25% CPU loading if fully loading one physical logical processor.

If a virtual terminal server is restarted due to installation of Microsoft patches, a higher number of users of the terminal server results in more disruption.

Thin Clients

These are small computers that normally have an embedded version of Windows 7 pre-installed by the manufacture of the thin client.

One or more monitors, keyboard, mouse and networking are connected to the thin client. Thin client establishes communication with the virtual client using client

software such as Microsoft's Remote Desktop Client. Minimal configuration is required to configure thin client software. This makes it easy to replace the unit.

Thin clients may be initially configured for screen and power saving. For production systems, these features must be turned off.

As thin client is normally using a flash disk, configuration of the device requires the disk to be placed in read-write mode. This is described in the device user manual. Once the configuration is complete, the device must be returned to its read-only mode.

Currently, thin clients are designed with a single interface. Hence, network redundancy using 800xA RNRP is not possible. It is possible to use a standard approved 800xA workstation PC as a thin client. In this case, RNRP can be installed. Whist the advantages of a true thin client are lost, the workstation needs only minimal software installation and configuration. Hence, replacement becomes a much easier task.

Multiple Screen

Primary considerations for multiple screens are that the operating system in the virtual client supports multiple screens. They can provide higher levels of loading as there is more screen real estate to bring up more objects.

Table 11 summarizes the operating system requirements:

Table 11. Operating System Requirement

Clients	Windows
Virtual Client Operating System	Windows 2008 Server R2 Windows 7 Enterprise Windows 7 Ultimate
Thin Client Operating System	Windows 7

Limitations

Physical clients contains dedicated graphics processor to assist in rendering graphics. Dedicated graphics adapters are essential in graphics intensive computing such as game playing. The array of graphic cores in the graphics adapter is required to handle the various requirements for presenting the graphics in these cases.

ABB 800xA systems are not gaming environments; however, their graphics resource usage varies based on user interaction. One area that produces high levels of loading in virtual clients and should therefore be avoided is the use of Process Graphics animated graphics. Examples are the Process Graphics Roll, Process Graphics Trend, and Process Graphics Rolling text.

When using the remote desktop to a virtual client or terminal server, Process Graphics Trend Ruler functionality is unpredictable.

Appendix A ESX(i) Host Setup Check List

Item	Setting	ESX1	ESX2
BIOS VT	Enabled		
BIOS VT-d	Enabled		
BIOS Execution	Enabled		
Hyper Threading	Enabled		
Hard Disk Configuration	Setup as RAID1 or RAID5		
Time	Correct local time		
Only vSphere Client	Connected		
All vSwitches	Gigabit Connection		

Appendix B ESX(i) Guest Setup Check List

Item	Setting	Guest1	Guest2	Guest3	Guest4
Machine Name	Note: No spaces				
Virtual Machine Version	7				
Guest OS	Windows 2008 or Windows 7				
No. of virtual processors	2				
Memory	4GB				
Virtual Network Adapter (E1000 only)	Based on documentation				
SCSI Controller	Use default				
Hard Disk	Based on node requirements				
Disk Provisioning	Thick				
Mode	Independent de-selected				
Video RAM	64MB				
Floppy drive	Removed				
VMware Tools	Installed				
Graphics Acceleration in Guest	Full				

Appendix C Further Technical Information on VMware ESX(i)

VMware ESX(i) normally requires a support agreement to be able to provide the required support.

The following links to a searchable VMware database for all technical documentation on VMware ESX:

http://www.vmware.com/resources/techresources/cat/91

The following links to a technically oriented forum hosted by VMware. Threads are answered by VMware ESX engineers, often within the same day. It is highly possible that common VMware ESX issues that the user may have already have been discussed and solved in this forum by others.

http://communities.vmware.com/community/vmtn/vsphere?view=discussions

Index

Numerics

64bit processor 28
800xA for Advant Master 27
800xA for MOD 300 27
800xA Licensing Dongle 25
800xA server
    Installation
        Configuration 31

A

ABB USB Dongle 26
About This User Manual 11
Adding a Datacenter Object 112
Adding an ESX Server 112
Aspect Servers 17
Asset Optimization Server 17

B

Backup and Restore of an ESX Server 43
Backup and Restore of Virtual Machines 44

C

Configuring vCenter Server 112
Configuring VMware High Availability 116
Connecting the 800xA USB Licensing Dongle to the CLS Server 25
Console Operating System 28
Consolidated 800xA System 18
Create Virtual Switches 38
Create VMs and Connect them to Virtual Switches 40

D

Determine Additional Hardware 25
Determine Required VMware ESX Server Hardware 22
Domain Controllers 17

E

ESX 4.1 11
ESX Server Network Configuration 101

I

Information Management Server 17
Install 800xA into the VMs 41
Installation Procedure 110
Installing vCenter Server 110
Installing vSphere Client 111

L

Limitations when Interacting with ESX Servers 113

M

Monitoring VMware vSphere ESX 11

N

Network Adapter 32
Non-virtualized 800xA System 17
non-virtualized system 19

O

Overview of Virtualization 15

P

Pre-requisites 110
PU410 27
PU412 27

S

SAN Hardware 94
SAN Networking 96
SAN Storage Configuration 95
service console 28
Set Up 800xA Server Nodes as VMs 38
    Create virtual switches 38
Setting ESX time 37
Storage Area Network (SAN) 93
System Planning 21

T

Total CPUs 23
Total disks 23
Total Network Interface Cards (NIC) 23
Total RAM 22

V

virtualization 11
VMware ESX 11
VMware ESX 4.1 28
VMware ESX Server 28
VMware ESX Server Installation 31
VMware ESX/ESXi 4.1 28
VMware ESXi Server 28
VMware ESXi Server Installation 34
VMware Fault Tolerance 120
VMware High Availability 115
VMware Storage vMotion 119
VMware vCenter Server 107
VMware vMotion 119
vSphere Client Installation 36

Revision History

This section provides information on the revision history of this User Manual.

The revision index of this User Manual is not related to the 800xA 5.1 System Revision.

The following table lists the revision history of this User Manual.

Revision Index	Description	Date
-	First version published for 800xA 5.1	June 2010
A	Updated for 800xA 5.1 Revision A release	May 2011
B	Updated for 800xA 5.1 Feature Pack release	August 2011
C	Updated for 800xA 5.1 64 bit release	November 2011
D	Updated for 800xA 5.1 Revision B release	June 2012
E	Updated for 800xA 5.1 Feature Pack 3 release	August 2012
F	Updated for 800xA 5.1 Feature Pack 4 release	February 2013

Updates in Revision Index A

The following table shows the updates made in this User Manual for 800xA 5.1 Rev A.

Updated Section/Subsection	Description of Update
Appendix A and Appendix B	Updated the Tables in Appendix A and Appendix B respectively.
Section 3, Advant Master and Advant MOD	Text removed in subsection *Advant Master and Advant MOD*.
Various Sections	Minor changes made throughout the manual.
Section 5, Backup and Restore	Text removed in subsection *Backup and Restore of an ESX Server*.
Section 10, Upgrading ESX 4.0 Update 1 to ESX 4.1	Text removed in subsection *Changes from ESX 4.0 Update1 to ESX 4.1.*

Updates in Revision Index B

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack.

Updated Section/Subsection	Description of Update
Section 12, Storage Area Network	Modified and updated the Section.
Section 13, VMware vCenter Server	Added the new section.
Section 14, Improving Availability	Added the new section.
Section 15, 800xA in the IT Infrastructure	Added the new section.
Section 16, Further Technical Information on VMware ESX	Section number is changed.
Section 3, Planning	Updated minor formatting issues.

Updated Section/Subsection	Description of Update
Section 8 Monitoring VMware vSphere ESX	Updated minor formatting issues. In the subsection *Adding ABB Object types* added the information.
Section 11 Supported 800xA Server Node Types	Updated subsection *Connectivities*.
Appendix A	Minor changes are done in the Appendix.
Various Sections	Minor changes made throughout the manual.
Index	Added the new section *Index*.

Updates in Revision Index C

The following table shows the updates made in this User Manual for 800xA 5.1 64-bit.

Updated Section/Subsection	Description of Update
Section 4 Installation and Configuration	Changes done in the subsection Install 800xA into the VMs.

Updates in Revision Index D

The following table shows the updates made in this User Manual for 800xA 5.1 Revision B release.

Updated Section/Subsection	Description of Update
Section 8 Monitoring VMware vSphere ESX	Added Monitoring SNMP Traps in ESXi Server subsection. Changes in the Install and Configure HP System Management in the ESX Server subsection in the Information Note at the end of the section. Minor changes updated in this section.
Section 4 Installation and Configuration	Added VMware ESXi Server Installation subsection. Changed Heading from VMware ESXi Server Installation to VMware ESXi 4.1 Server Installation. Information icon is added for License issue. Minor changes in vSphere Client Installation subsection.
All Sections	Renamed ESX/ESXi to ESX(i).
Section 3 Planning	Minor changes in Determine Required VMware ESX(i) Server Hardware subsection.

Updates in Revision Index E

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 3 release.

Updated Section/Subsection	Description of Update
Section 11 Supported 800xA Server Node Types	Updated *Connectivities* subsection.

Updates in Revision Index F

The following table shows the updates made in this User Manual for 800xA 5.1 Feature Pack 4 release.

Updated Section/Subsection	Description of Update
Section 16 Virtual Client	Newly added section. Changes updated to the section.
Appendix C Further Technical Information on VMware ESX(i)	Changed Section 16 Further Technical Information on VMware ESX(i) to Appendix C Further Technical Information on VMware ESX(i).
Section 3 Planning	Updates to the VMware vSphere ESX Versions subsection.
Section 4 Installation and Configuration	Renamed VMware ESXi Server Installation to VMware ESXi 5.0 Server Installation. Added a caution in the Create VMs and Connect them to Virtual Switches subsection.
Section 11 Supported 800xA Server Node Types	Updated the following subsections: • Redundant 4 Node 800xA System • Redundant 8 Node 800xA System
Appendix B ESX(i) Guest Setup Check List	Updated the changes to the section.
Section 8 Monitoring VMware vSphere ESX	Updated the Supported Hardware for Virtualization subsection. Updated Monitoring SNMP Traps in ESXi Server subsection.
Rename the User Manual	Server Node Virtualization User Manual is renamed to Virtualization. **System 800xA Server Node Virtualization** to **System 800xA Virtualization**.

Contact us

ABB AB
Control Technologies
Västerås, Sweden
Phone: +46 (0) 21 32 50 00
e-mail: processautomation@se.abb.com
www.abb.com/controlsystems

ABB Automation GmbH
Control Technologies
Mannheim, Germany
Phone: +49 1805 26 67 76
e-mail: marketing.control-products@de.abb.com
www.abb.de/controlsystems

ABB S.P.A.
Control Technologies
Sesto San Giovanni (MI), Italy
Phone: +39 02 24147 555
e-mail: controlsystems@it.abb.com
www.abb.it/controlsystems

ABB Inc.
Control Technologies
Wickliffe, Ohio, USA
Phone: +1 440 585 8500
e-mail: industrialitsolutions@us.abb.com
www.abb.com/controlsystems

ABB Pte Ltd
Control Technologies
Singapore
Phone: +65 6776 5711
e-mail: processautomation@sg.abb.com
www.abb.com/controlsystems

ABB Automation LLC
Control Technologies
Abu Dhabi, United Arab Emirates
Phone: +971 (0) 2 4938 000
e-mail: processautomation@ae.abb.com
www.abb.com/controlsystems

ABB China Ltd
Control Technologies
Beijing, China
Phone: +86 (0) 10 84566688-2193
www.abb.com/controlsystems

3BSE056141-510 F

Copyright © 2003-2013 by ABB.
All rights reserved.

Power and productivity
for a better world™